

PATENT COOPERATION TREATY

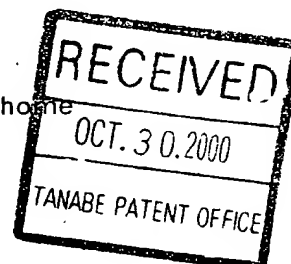
PCT

NOTICE INFORMING THE APPLICANT OF THE
COMMUNICATION OF THE INTERNATIONAL
APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

From the INTERNATIONAL BUREAU

To:

TANABE, Shigemoto
Green-Fantasia Building
5th floor
11-11-508, Jingumae 1-cho
Shibuya-ku
Tokyo 150-0001
JAPON

Date of mailing (day/month/year) 19 October 2000 (19.10.00)		
Applicant's or agent's file reference S00P0777WO00		IMPORTANT NOTICE
International application No. PCT/JP00/02290	International filing date (day/month/year) 07 April 2000 (07.04.00)	
		Priority date (day/month/year) 12 April 1999 (12.04.99)
Applicant SONY CORPORATION et al		

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:

KR,US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:

CN,EP,SG

The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on 19 October 2000 (19.10.00) under No. WO 00/62217

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a demand for international preliminary examination must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the national phase, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer J. Zahra
Facsimile No. (41-22) 740.14.35	Telephone No. (41-22) 338.83.38

This Page Blank (uspto)

特 許 協 力 条 約

発信人 日本国特許庁 (国際調査機関)

出願人代理人

田辺 恵基



殿

あて名

〒 150-0001

S745W0

東京都渋谷区神宮前1丁目11番11-508号
グリーンフアンタジアビル5階
田辺特許事務所

PCT

国際調査報告又は国際調査報告を作成しない旨
の決定の送付の通知書

(法施行規則第41条)
(PCT規則44.1)

発送日
(日.月.年)

13.06.00

出願人又は代理人
の書類記号

S00P0777WO00

今後の手続きについては、下記1及び4を参照。

国際出願番号

PCT/JP00/02290

国際出願日
(日.月.年)

07.04.00

出願人 (氏名又は名称)

ソニー株式会社

1. ☒ 国際調査報告が作成されたこと、及びこの送付書とともに送付することを、出願人に通知する。

PCT19条の規定に基づく補正書及び説明書の提出

出願人は、国際出願の請求の範囲を補正することができる (PCT規則46参照)。

いつ 補正書の提出期間は、通常国際調査報告の送付の日から2月である。

詳細については添付用紙の備考を参照すること。

どこへ 直接次の場所へ

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22) 740.14.35

詳細な手続については、添付用紙の備考を参照すること。

2. ☐ 国際調査報告が作成されないこと、及び法第8条第2項 (PCT17条(2)(a)) の規定による国際調査報告を作成しない旨の決定をこの送付書とともに送付することを、出願人に通知する。

3. ☐ 法施行規則第44条 (PCT規則40.2) に規定する追加手数料の納付に対する異議の申立てに関して、出願人に下記の点を通知する。

☐ 異議の申立てと当該異議についての決定を、その異議の申し立てと当該異議についての決定の両方を指定官庁へ送付することを求める出願人の請求とともに、国際事務局へ送付した。

☐ 当該異議についての決定は、まだ行われていない。決定されしだい出願人に通知する。

4. 今後の手続： 出願人は次の点に注意すること。

優先日から18月経過後、国際出願は国際事務局によりすみやかに国際公開される。出願人が公開の延期を望むときは、国際出願又は優先権の主張の取下げの通知がPCT規則90の2.1及び90の2.3にそれぞれ規定されているように、国際公開の事務的な準備が完了する前に国際事務局に到達しなければならない。

出願人が優先日から30月まで (官庁によってはもっと遅く) 国内段階の開始を延期することを望むときは、優先日から19月以内に、国際予備審査の請求書が提出されなければならない。

国際予備審査の請求書若しくは、後にする選択により優先日から19箇月以内に選択しなかった又は第二章に拘束されないため選択できなかったすべての指定官庁に対しては優先日から20月以内に、国内段階の開始のための所定手続を取らなければならない。

名称及びあて名

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

権限のある職員

特 許 庁 長 官

5 L

9 2 8 7

電話番号 03-3581-1101 内線 3562

This Page Blank (uspto)

注 意

1. 国際調査報告の発送日から起算する条約第19条(1)及び規則46.1に従う国際事務局への補正期間に注意してください。
2. 条約22条(2)に規定する期間に注意してください。

3. 文献の写しの請求について

国際調査報告に記載した文献の複写

特許庁にこれらの引用文献の写しを請求することもできますが、日本特許情報機構でもこれらの引用文献の複写物を販売しています。日本特許情報機構に引用文献の複写物を請求する場合は下記の点に注意してください。

〔申込方法〕

(1) 特許(実用新案・意匠)公報については、下記の点を明記してください。

○特許・実用新案及び意匠の種類

○出願公告又は出願公開の年次及び番号(又は特許番号、登録番号)

○必要部数

(2) 公報以外の文献の場合は、下記の点に注意してください。

○国際調査報告の写しを添付してください(返却します)。

〔申込み及び照会先〕

〒135 東京都江東区東陽4-1-7 佐藤ダイヤビル

財団法人 日本特許情報機構 サービス課

TEL 03-5690-3900

注意 特許庁に対して文献の写しの請求をすることができる期間は、国際出願日から7年です。

This Page Blank (uspto)

様式PCT/ISA/220の備考

この備考は、PCT 19条の規定に基づく補正書の提出に関する基本的な指示を与えるためのものである。この備考は特許協力条約並びにこの条約に基づく規則及び実施細則の規定に基づいている。この備考とそれらの規定とが相違する場合には、後者が適用される。詳細な情報については、WIPOの出版物であるPCT出願人の手引も参照すること。

PCT 19条の規定に基づく補正書の提出に関する指示

出願人は、国際調査報告を受領した後、国際出願の請求の範囲を補正する機会が一回ある。しかし、国際出願のすべての部分（請求の範囲、明細書及び図面）が、国際予備審査の手續においても補正できるもので、例えば出願人が仮保護のために補正書を公開することを希望する場合又は国際公開前に請求の範囲を補正する別の理由がある場合を除き、通常PCT 19条の規定に基づく補正書を提出する必要はないことを強調しておく。さらに、仮保護は一部の国のみで与えられるだけであることも強調しておく。

補正の対象となるもの

PCT 19条の規定により請求の範囲のみ補正することができる。

国際段階においてPCT 34条の規定に基づく国際予備審査の手續において請求の範囲を（更に）補正することができる。

明細書及び図面は、PCT 34条の規定に基づく国際予備審査の手續においてのみ補正することができる。

国内段階に移行する際、PCT 28条（又はPCT 41条）の規定により、国際出願のすべての部分を補正することができる。

いつ

国際調査報告の送付の日から2月又は優先日から16月の内どちらか遅く満了するほうの期間内。しかし、その期間の満了後であっても国際公開の技術的な準備の完了前に国際事務局が補正を受領した場合には、その補正書は、期間内に受理されたものとみなすことを強調しておく（PCT規則46.1）。

補正書を提出すべきところ

補正書は、国際事務局のみに提出でき、受理官庁又は国際調査機関には提出してはいけない（PCT規則46.2）。国際予備審査の請求書を提出した／する場合については、以下を参照すること。

どのように

1以上の請求の範囲の削除、1以上の新たな請求の範囲の追加、又は1以上の請求の範囲の記載の補正による。

差替え用紙は、補正の結果、出願当初の用紙と相違する請求の範囲の各用紙毎に提出する。

差替え用紙に記載されているすべての請求の範囲には、アラビア数字を付さなければならない。請求の範囲を削除する場合、その他の請求の範囲の番号を付け直す必要はない。請求の範囲の番号を付け直す場合には、連続番号で付け直すなければならない（PCT実施細則第205号(b)）。

補正は国際公開の言語で行う。

補正書にどのような書類を添付しなければならないか

書簡（PCT実施細則第205号(b)）

補正書には書簡を添付しなければならない。

書簡は国際出願及び補正された請求の範囲とともに公開されることはない。これを「PCT 19条(1)に規定する説明書」と混同してはならない（「PCT 19条(1)に規定する説明書」については、以下を参照）。

書簡は、英語又は仏語を選択しなければならない。ただし、国際出願の言語が英語の場合、書簡は英語で、仏語の場合、書簡は仏語で記載しなければならない。

書簡には、出願時の請求の範囲と補正された請求の範囲との相違について表示しなければならない。特に、国際出願に記載した各請求の範囲との関連で次の表示（2以上の請求の範囲についての同一の表示する場合は、まとめることができる。）をしなければならない。

- (i) この請求の範囲は変更しない。
- (ii) この請求の範囲は削除する。
- (iii) この請求の範囲は追加である。
- (iv) この請求の範囲は出願時の1以上の請求の範囲と差し替える。
- (v) この請求の範囲は出願時の請求の範囲の分割の結果である。

This Page Blank (uspto)

次に、添付する書簡中での、補正についての説明の例を示す。

1. [請求の範囲の一部の補正によって請求の範囲の項数が48から51になった場合] :
“請求の範囲1-29、31、32、34、35、37-48項は、同じ番号のもとに補正された請求の範囲と置き換えられた。請求の範囲30、33及び36項は変更なし。新たに請求の範囲49-51項が追加された。”
2. [請求の範囲の全部の補正によって請求の範囲の項数が15から11になった場合] :
“請求の範囲1-15項は、補正された請求の範囲1-11項に置き換えられた。”
3. [原請求の範囲の項数が14で、補正が一部の請求の範囲の削除と新たな請求の範囲の追加を含む場合] :
“請求の範囲1-6及び14項は変更なし。請求の範囲7-13は削除。新たに請求の範囲15、16及び17項を追加。”又は
“請求の範囲7-13は削除。新たに請求の範囲15、16及び17項を追加。その他の全ての請求の範囲は変更なし。”
4. [各種の補正がある場合] :
“請求の範囲1-10項は変更なし。請求の範囲11-13、18及び19項は削除。請求の範囲14、15及び16項は補正された請求の範囲14項に置き換えられた。請求の範囲17項は補正された請求の範囲15、16及び17項に分割された。新たに請求の範囲20及び21項が追加された。”

“PCT19条(1)の規定に基づく説明書”(PCT規則46.4)

補正書には、補正並びにその補正が明細書及び図面に与える影響についての説明書を提出することができる(明細書及び図面はPCT19条(1)の規定に基づいては補正できない)。

説明書は、国際出願及び補正された請求の範囲とともに公開される。

説明書は、国際公開の言語で作成しなければならない。

説明書は、簡潔でなければならない、英語の場合又は英語に翻訳した場合に500語を越えてはならない。

説明書は、出願時の請求の範囲と補正された請求の範囲との相違を示す書簡と混同してはならない。説明書を、その書簡に代えることはできない。説明書は別紙で提出しなければならない、見出しを付すものとし、その見出しは“PCT19条(1)の規定に基づく説明書”の語句を用いることが望ましい。

説明書には、国際調査報告又は国際調査報告に列記された文献との関連性に関して、これらを誹謗する意見を記載してはならない。国際調査報告に列記された特定の請求の範囲に関連する文献についての言及は、当該請求の範囲の補正に関してのみ行うことができる。

国際予備審査の請求書が提出されている場合

PCT19条の規定に基づく補正書及び添付する説明書の提出の時に国際予備審査の請求書が既に提出されている場合には、出願人は、補正書(及び説明書)を国際事務局に提出すると同時にその写し及び必要な場合、その翻訳文を国際予備審査機関にも提出することが望ましい(PCT規則55.3(a)、62.2の第1文を参照)。詳細は国際予備審査請求書(PCT/ISA/401)の注意書参照。

国内段階に移行するための国際出願の翻訳に関して

国内段階に移行する際、PCT19条の規定に基づいて補正された請求の範囲の翻訳を出願時の請求の範囲の翻訳の代わりに又は追加して、指定官庁/選択官庁に提出しなければならないこともあるので、出願人は注意されたい。

指定官庁/選択官庁の詳細な要求については、PCT出願人の手引きの第II巻を参照。

This Page Blank (uspto)

P C T

国際調査報告

(法 8 条、法施行規則第40、41条)
〔P C T 1 8 条、P C T 規則43、44〕

出願人又は代理人 の書類記号 S 0 0 P 0 7 7 7 W O 0 0	今後の手続きについては、国際調査報告の送付通知様式(P C T / I S A / 2 2 0) 及び下記 5 を参照すること。		
国際出願番号 P C T / J P 0 0 / 0 2 2 9 0	国際出願日 (日.月.年) 0 7 . 0 4 . 0 0	優先日 (日.月.年) 1 2 . 0 4 . 9 9	
出願人 (氏名又は名称) ソニー株式会社			

国際調査機関が作成したこの国際調査報告を法施行規則第41条 (P C T 1 8 条) の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 2 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない (第 I 欄参照)。

3. ☐ 発明の単一性が欠如している (第 II 欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。

☐ 第 III 欄に示されているように、法施行規則第47条 (P C T 規則38.2(b)) の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から 1 カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、
第 1 3 図とする。 ☒ 出願人が示したとおりである。

☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

This Page Blank (uspto)

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F17/60

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F17/60 G06F13/00 G09C1/00 H04L9/08 G06F15/00 H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年

日本国公開実用新案公報 1971-2000年

日本国実用新案登録公報 1996-2000年

日本国登録実用新案公報 1994-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル(JOIS)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	WO, 96/27155, A2 (InerTrust Technologies Corp.) 6.9月. 1996 (06.09.96) & JP, 10-512074, A	1-8
Y	人文科学とコンピュータ, 第36-8巻, 11月. 1997 河原正治「著作権処理技術の最近の動向」 p. 43-48	1-8

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

24.05.00

国際調査報告の発送日

13.06.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

岩間 直純



5L

9287

電話番号 03-3581-1101 内線 3562

This Page Blank (uspto)

PATENT COOPERATION TREATY

PCT

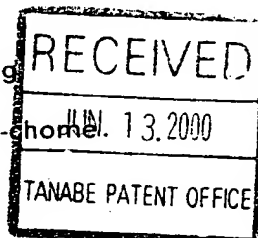
NOTIFICATION OF RECEIPT OF
RECORD COPY

(PCT Rule 24.2(a))

From the INTERNATIONAL BUREAU

To:

TANABE, Shigemoto
Green-Fantasia Building
5th floor
11-11-508, Jingumae 1-chome
Shibuya-ku
Tokyo 150-0001
JAPON



Date of mailing (day/month/year) 01 May 2000 (01.05.00)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference S00P0777WO00	International application No. PCT/JP00/02290

The applicant is hereby notified that the International Bureau has received the record copy of the international application as detailed below.

Name(s) of the applicant(s) and State(s) for which they are applicants:

SONY CORPORATION (for all designated States except US)
ISHIBASHI, Yoshihito (for US)

International filing date : 07 April 2000 (07.04.00)
Priority date(s) claimed : 12 April 1999 (12.04.99)
Date of receipt of the record copy : 26 April 2000 (26.04.00)
by the International Bureau :
List of designated Offices :

EP : DE, FR, GB
National : CN, KR, SG, US

ATTENTION

The applicant should carefully check the data appearing in this Notification. In case of any discrepancy between these data and the indications in the international application, the applicant should immediately inform the International Bureau.

In addition, the applicant's attention is drawn to the information contained in the Annex, relating to:

- ☒ time limits for entry into the national phase
- ☒ confirmation of precautionary designations
- ☒ requirements regarding priority documents

A copy of this Notification is being sent to the receiving Office and to the International Searching Authority.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. (41-22) 740.14.35	Authorized officer: Y. KUWAHARA Telephone No. (41-22) 338.83.38
--	---

This Page Blank (uspto)

INFORMATION ON TIME LIMITS FOR ENTERING THE NATIONAL PHASE

The applicant is reminded that the "national phase" must be entered before each of the designated Offices indicated in the Notification of Receipt of Record Copy (Form PCT/IB/301) by paying national fees and furnishing translations, as prescribed by the applicable national laws.

The time limit for performing these procedural acts is **20 MONTHS** from the priority date or, for those designated States which the applicant elects in a demand for international preliminary examination or in a later election, **30 MONTHS** from the priority date, provided that the election is made before the expiration of 19 months from the priority date. Some designated (or elected) Offices have fixed time limits which expire even later than 20 or 30 months from the priority date. In other Offices an extension of time or grace period, in some cases upon payment of an additional fee, is available.

In addition to these procedural acts, the applicant may also have to comply with other special requirements applicable in certain Offices. It is the applicant's responsibility to ensure that the necessary steps to enter the national phase are taken in a timely fashion. Most designated Offices do not issue reminders to applicants in connection with the entry into the national phase.

For detailed information about the procedural acts to be performed to enter the national phase before each designated Office, the applicable time limits and possible extensions of time or grace periods, and any other requirements, see the relevant Chapters of Volume II of the PCT Applicant's Guide. Information about the requirements for filing a demand for international preliminary examination is set out in Chapter IX of Volume I of the PCT Applicant's Guide.

GR and ES became bound by PCT Chapter II on 7 September 1996 and 6 September 1997, respectively, and may, therefore, be elected in a demand or a later election filed on or after 7 September 1996 and 6 September 1997, respectively, regardless of the filing date of the international application. (See second paragraph above.)

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

CONFIRMATION OF PRECAUTIONARY DESIGNATIONS

This notification lists only specific designations made under Rule 4.9(a) in the request. It is important to check that these designations are correct. Errors in designations can be corrected where precautionary designations have been made under Rule 4.9(b). The applicant is hereby reminded that any precautionary designations may be confirmed according to Rule 4.9(c) before the expiration of 15 months from the priority date. If it is not confirmed, it will automatically be regarded as withdrawn by the applicant. There will be no reminder and no invitation. Confirmation of a designation consists of the filing of a notice specifying the designated State concerned (with an indication of the kind of protection or treatment desired) and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.

REQUIREMENTS REGARDING PRIORITY DOCUMENTS

For applicants who have not yet complied with the requirements regarding priority documents, the following is recalled.

Where the priority of an earlier national, regional or international application is claimed, the applicant must submit a copy of the said earlier application, certified by the authority with which it was filed ("the priority document") to the receiving Office (which will transmit it to the International Bureau) or directly to the International Bureau, before the expiration of 16 months from the priority date, provided that any such priority document may still be submitted to the International Bureau before that date of international publication of the international application, in which case that document will be considered to have been received by the International Bureau on the last day of the 16-month time limit (Rule 17.1(a)).

Where the priority document is issued by the receiving Office, the applicant may, instead of submitting the priority document, request the receiving Office to prepare and transmit the priority document to the International Bureau. Such request must be made before the expiration of the 16-month time limit and may be subjected by the receiving Office to the payment of a fee (Rule 17.1(b)).

If the priority document concerned is not submitted to the International Bureau or if the request to the receiving Office to prepare and transmit the priority document has not been made (and the corresponding fee, if any, paid) within the applicable time limit indicated under the preceding paragraphs, any designated State may disregard the priority claim, provided that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity to furnish the priority document within a time limit which is reasonable under the circumstances.

Where several priorities are claimed, the priority date to be considered for the purposes of computing the 16-month time limit is the filing date of the earliest application whose priority is claimed.

This Page Blank (uspto)

PCT COOPERATION TREATY

PCT

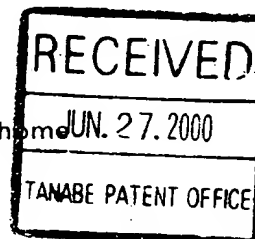
NOTIFICATION CONCERNING
SUBMISSION OR TRANSMITTAL
OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

From the INTERNATIONAL BUREAU

To:

TANABE, Shigemoto
Green-Fantasia Building
5th floor
11-11-508, Jingumae 1-chome
Shibuya-ku
Tokyo 150-0001
JAPON



5745WO

Date of mailing (day/month/year) 08 June 2000 (08.06.00)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference S00P0777WO00	
International application No. PCT/JP00/02290	International filing date (day/month/year) 07 April 2000 (07.04.00)
International publication date (day/month/year) Not yet published	Priority date (day/month/year) 12 April 1999 (12.04.99)
Applicant SONY CORPORATION et al	

- The applicant is hereby notified of the date of receipt (except where the letters "NR" appear in the right-hand column) by the International Bureau of the priority document(s) relating to the earlier application(s) indicated below. Unless otherwise indicated by an asterisk appearing next to a date of receipt, or by the letters "NR", in the right-hand column, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).
- This updates and replaces any previously issued notification concerning submission or transmittal of priority documents.
- An asterisk(*) appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b). In such a case, the attention of the applicant is directed to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.
- The letters "NR" appearing in the right-hand column denote a priority document which was not received by the International Bureau or which the applicant did not request the receiving Office to prepare and transmit to the International Bureau, as provided by Rule 17.1(a) or (b), respectively. In such a case, the attention of the applicant is directed to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

<u>Priority date</u>	<u>Priority application No.</u>	<u>Country or regional Office or PCT receiving Office</u>	<u>Date of receipt of priority document</u>
12 Apr 1999 (12.04.99)	11/103992	JP	26 May 2000 (26.05.00)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer

Somsak Thiphrakesone

Telephone No. (41-22) 338.83.38

This Page Blank (uspto)

特許協力条約に基づく国際出願

願 書

出願人は、この国際出願が特許協力条約に従って処理されることを請求する。

国際出願番号

PCT

国際出願日

07.4.00

(受付印)

受領印

出願人又は代理人の登録記号
(希望する場合、最大12字)

S 00 P 0777 W O 00

第 I 欄 発明の名称

情報処理装置および方法、並びに提供媒体

第 II 欄 出願人

氏名(名称)及びあて名:(姓・名の順に記載;法人は公式の完全な名称を記載;あて名は郵便番号及び国名も記載)

ソニー株式会社

SONY CORPORATION

〒141-0001 日本国東京都品川区北品川6丁目7番35号

7-35, Kitashinagawa 6-chome, Shinagawa-ku, TOKYO 141-0001, JAPAN

☐ この欄に記載した者は、
発明者でもある。

電話番号:

03-5448-2617

ファクシミリ番号:

03-5448-3063

加入電話番号:

J22262

国籍(国名): 日本国 JAPAN

住所(国名): 日本国 JAPAN

この欄に記載した者は、次の
指定国についての出願人である:

☐ すべての指定国

☒ 米国を除くすべての指定国

☐ 米国のみ

☐ 追記欄に記載した指定国

第 III 欄 その他の出願人又は発明者

氏名(名称)及びあて名:(姓・名の順に記載;法人は公式の完全な名称を記載;あて名は郵便番号及び国名も記載)

石橋 義人

ISHIBASHI Yoshihito

〒141-0001 日本国東京都品川区北品川6丁目7番35号

ソニー株式会社内

C/O SONY CORPORATION, 7-35, Kitashinagawa 6-chome,
Shinagawa-ku, TOKYO 141-0001, JAPAN

この欄に記載した者は
次に該当する:

☐ 出願人のみである。

☒ 出願人及び発明者である。

☐ 発明者のみである。
(ここにレ印を付したとき
は、以下に記入しないこと)

国籍(国名): 日本国 JAPAN

住所(国名): 日本国 JAPAN

この欄に記載した者は、次の
指定国についての出願人である:

☐ すべての指定国

☐ 米国を除くすべての指定国

☒ 米国のみ

☐ 追記欄に記載した指定国

☐ その他の出願人又は発明者が続葉に記載されている。

第 IV 欄 代理人又は共通の代表者、通知のあて名

次に記載された者は、国際機関において出願人のために行動する:

☒ 代理人

☐ 共通の代表者

氏名(名称)及びあて名:(姓・名の順に記載;法人は公式の完全な名称を記載;あて名は郵便番号及び国名も記載)

8274 弁理士 田 辺 恵 基

TANABE Shigemoto

〒150-0001 日本国東京都渋谷区神宮前1丁目11番11-508号
グリーンファンタジアビル5階

Green-Fantasia Building 5th Floor, 11-11-508,
Jingumae 1-chome, Shibuya-ku, TOKYO 150-0001, JAPAN

電話番号:

03-3470-6591

ファクシミリ番号:

03-3470-6506

加入電話番号:

通知のためのあて名: 代理人又は共通の代表者が選任されておらず、上記枠内に特に通知が送付されるあて名を記載している場合は、レ印を付す。

This Page Blank (uspto)

第Ⅴ欄 国の指定

規則 4.9(a)の規定に基づき次の指定を行う（記入する□にレ印を付すこと：少なくとも1つの□にレ印を付すこと）。

広域半島国

- ☐ **AP** **ARIPPO** 半島国：GH ガーナ Ghana, GM ガンビア Gambia, KE ケニア Kenya, LS レント Lesotho, MW マラウイ Malawi, SD スーダン Sudan, SL シエラ・レオネ Sierra Leone, SZ スワジランド Swaziland, TZ タンザニア United Republic of Tanzania, UG ウガンダ Uganda, ZW ジンバブエ Zimbabwe, 及びハラレプロトコルと特許協力条約の締結国である他の国
- ☐ **EA** ユーラシア半島国：AM アルメニア Armenia, AZ アゼルバイジャン Azerbaijan, BY ベラルーシ Belarus, KG キルギス Kyrgyzstan, KZ カザフスタン Kazakhstan, MD モルドヴァ Republic of Moldova, RU ロシア Russian Federation, TJ タジキスタン Tajikistan, TM トルクメニスタン Turkmenistan, 及びユーラシア特許条約と特許協力条約の締結国である他の国
- ☒ **EP** ヨーロッパ半島国：~~AT オーストリア Austria, BE ベルギー Belgium, CH and LI スイス及びリヒテンシュタイン Switzerland and Liechtenstein, CY キプロス Cyprus, DE ドイツ Germany, DK デンマーク Denmark, ES スペイン Spain, FI フィンランド Finland, FR フランス France, GB 英国 United Kingdom, GR ギリシャ Greece, IE アイルランド Ireland, IT イタリア Italy, LU ルクセンブルグ Luxembourg, MC モナコ Monaco, NL オランダ Netherlands, PT ポルトガル Portugal, SE スウェーデン Sweden,~~ 及びヨーロッパ特許条約と特許協力条約の締結国である他の国
- ☐ **OA** **OAPI** 半島国：BF ブルキナ・ファソ Burkina Faso, BJ ベナン Benin, CF 中央アフリカ Central African Republic, CG コンゴ Congo, CI コートジボアール Côte d'Ivoire, CM カメルーン Cameroon, GA ガボン Gabon, GN ギニア Guinea, GW ギニア・ビサウ Guinea-Bissau, ML マリ Mali, MR モリタニア Mauritania, NE ニジェール Niger, SN セネガル Senegal, TD チャード Chad, TG トーゴ Togo, 及びアフリカ知的財産権機構のメンバー国と特許協力条約の締結国である他の国（他の種類の保護又は取扱いを求める場合には点線の上に記載する）

国（内）半島国（他の種類の保護又は取扱いを求める場合には点線の上に記載する）

- | | |
|--|--|
| <input type="checkbox"/> AE アラブ首長国連邦 United Arab Emirates | <input type="checkbox"/> LR リベリア Liberia |
| <input type="checkbox"/> AL アルバニア Albania | <input type="checkbox"/> LS レント Lesotho |
| <input type="checkbox"/> AM アルメニア Armenia | <input type="checkbox"/> LT リトアニア Lithuania |
| <input type="checkbox"/> AT オーストリア Austria | <input type="checkbox"/> LU ルクセンブルグ Luxembourg |
| <input type="checkbox"/> AU オーストラリア Australia | <input type="checkbox"/> LV ラトヴィア Latvia |
| <input type="checkbox"/> AZ アゼルバイジャン Azerbaijan | <input type="checkbox"/> MA モロッコ Morocco |
| <input type="checkbox"/> BA ボスニア・ヘルツェゴヴィナ Bosnia and Herzegovina | <input type="checkbox"/> MD モルドヴァ Republic of Moldova |
| <input type="checkbox"/> BB バルバドス Barbados | <input type="checkbox"/> MG マダガスカル Madagascar |
| <input type="checkbox"/> BG ブルガリア Bulgaria | <input type="checkbox"/> MK マケドニア旧ユーゴスラヴィア共和国 The former Yugoslav Republic of Macedonia |
| <input type="checkbox"/> BR ブラジル Brazil | <input type="checkbox"/> MN モンゴル Mongolia |
| <input type="checkbox"/> BY ベラルーシ Belarus | <input type="checkbox"/> MW マラウイ Malawi |
| <input type="checkbox"/> CA カナダ Canada | <input type="checkbox"/> MX メキシコ Mexico |
| <input type="checkbox"/> CH and LI スイス及びリヒテンシュタイン Switzerland and Liechtenstein | <input type="checkbox"/> NO ノルウェー Norway |
| <input checked="" type="checkbox"/> CN 中国 China | <input type="checkbox"/> NZ ニュー・ジージーランド New Zealand |
| <input type="checkbox"/> CR コスタリカ Costa Rica | <input type="checkbox"/> PL ポーランド Poland |
| <input type="checkbox"/> CU キューバ Cuba | <input type="checkbox"/> PT ポルトガル Portugal |
| <input type="checkbox"/> CZ チェッコ Czech Republic | <input type="checkbox"/> RO ルーマニア Romania |
| <input type="checkbox"/> DE ドイツ Germany | <input type="checkbox"/> RU ロシア Russian Federation |
| <input type="checkbox"/> DK デンマーク Denmark | <input type="checkbox"/> SD スーダン Sudan |
| <input type="checkbox"/> DM ドミニカ Dominica | <input type="checkbox"/> SE スウェーデン Sweden |
| <input type="checkbox"/> EE エストニア Estonia | <input checked="" type="checkbox"/> SG シンガポール Singapore |
| <input type="checkbox"/> ES スペイン Spain | <input type="checkbox"/> SI スロヴェニア Slovenia |
| <input type="checkbox"/> FI フィンランド Finland | <input type="checkbox"/> SK スロヴァキア Slovakia |
| <input type="checkbox"/> GB 英国 United Kingdom | <input type="checkbox"/> SL シエラ・レオネ Sierra Leone |
| <input type="checkbox"/> GD グレナダ Grenada | <input type="checkbox"/> TJ タジキスタン Tajikistan |
| <input type="checkbox"/> GE グルジア Georgia | <input type="checkbox"/> TM トルクメニスタン Turkmenistan |
| <input type="checkbox"/> GH ガーナ Ghana | <input type="checkbox"/> TR トルコ Turkey |
| <input type="checkbox"/> GM ガンビア Gambia | <input type="checkbox"/> TT トリニダード・トバゴ Trinidad and Tobago |
| <input type="checkbox"/> HR クロアチア Croatia | <input type="checkbox"/> TZ タンザニア United Republic of Tanzania |
| <input type="checkbox"/> HU ハンガリー Hungary | <input type="checkbox"/> UA ウクライナ Ukraine |
| <input type="checkbox"/> ID インドネシア Indonesia | <input type="checkbox"/> UG ウガンダ Uganda |
| <input type="checkbox"/> IL イスラエル Israel | <input checked="" type="checkbox"/> US 米国 United States of America |
| <input type="checkbox"/> IN インド India | <input type="checkbox"/> UZ ウズベキスタン Uzbekistan |
| <input type="checkbox"/> IS アイスランド Iceland | <input type="checkbox"/> VN ヴィエトナム Viet Nam |
| <input type="checkbox"/> JP 日本 Japan | <input type="checkbox"/> YU ユーゴスラヴィア Yugoslavia |
| <input type="checkbox"/> KE ケニア Kenya | <input type="checkbox"/> ZA 南アフリカ共和国 South Africa |
| <input type="checkbox"/> KG キルギス Kyrgyzstan | <input type="checkbox"/> ZW ジンバブエ Zimbabwe |
| <input type="checkbox"/> KP 北朝鮮 Democratic People's Republic of Korea | |
| <input checked="" type="checkbox"/> KR 韓国 Republic of Korea | |
| <input type="checkbox"/> KZ カザフスタン Kazakhstan | |
| <input type="checkbox"/> LC セント・ルシア Saint Lucia | |
| <input type="checkbox"/> LK スリ・ランカ Sri Lanka | |

下の□は、この様式の施行後に特許協力条約の締結国となった国を指定するためのものである

- ☐ _____
- ☐ _____
- ☐ _____

指定の確証の宣言：出願人は、上記の指定に加えて、規則 4.9(b)の規定に基づき、特許協力条約の下で認められる他の全ての国の指定を行う。ただし、この宣言から除く旨の表示を追記欄にした国は、指定から除かれる。出願人は、これらの追加される指定が確証を条件としていること、並びに優先日から15月が経過する前にその確証がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。（指定の確証（料金を含む）は、優先日から15月以内に受理官庁へ提出しなければならない。）

This Page Blank (uspto)

第VI欄 優先権主張

☐ 他の優先権の主張（先の出願）が追記欄に記載されている

先の出願日 (日. 月. 年)	先の出願番号	先の出願		
		国内出願 : 国名	広域出願 : *広域官庁名	国際出願 : 受理官庁名
(1) 12. 04. 99	平成11年特許願 第103992号	日本国 JAPAN		
(2)				
(3)				

☒ 上記()の番号の先の出願（ただし、本国際出願が提出される受理官庁に対して提出されたものに限る）のうち、次の()の番号のものについては、出願書類の認証原本を作成し国際事務局へ送付することを、受理官庁（日本国特許庁の長官）に対して請求している。 (1)

*先の出願が、ARIPOの特許出願である場合には、その先の出願を行った工業所有権の保護のためのパリ条約同盟国の少なくとも1ヶ国を追記欄に表示しなければならない（規則4.10(b)(ii)）。追記欄を参照。

第VII欄 国際調査機関

国際調査機関（ISA）の選択

先の調査結果の利用請求：当該調査の照会（先の調査が、国際調査機関によって既に実施又は請求されている場合）

出願日（日. 月. 年）

出願番号

国名（又は広域官庁）

ISA / JP

第VIII欄 照合欄：出願の言語

この国際出願の用紙の枚数は次のとおりである。

願書 3 枚
 明細書（配列表を除く） 71 枚
 請求の範囲 5 枚
 要約書 1 枚
 図面 50 枚
 明細書の配列表 0 枚
 合 計 130 枚

この国際出願には、以下にチェックした書類が添付されている。

- ☒ 手数料計算用紙
- ☒ 納付する手数料に相当する特許印紙を貼付した書面
- ☒ 国際事務局の口座への振込みを証明する書面
- ☐ 別個の記名押印された委任状
- ☐ 包括委任状の写し
- ☐ 記名押印（署名）の説明書
- ☐ 優先権書類（上記第VI欄の()の番号を記載する）
- ☐ 国際出願の翻訳文（翻訳に使用した言語名を記載する）
- ☐ 寄託した微生物又は他の生物材料に関する書面
- ☐ スクレオチド又はアミノ酸配列表（フレキシブルディスク）
- ☐ その他（書類名を詳細に記載する）

要約書とともに提示する図面： 13

本国際出願の使用言語名： 日本語

第IX欄 提出者の記名押印

各人の氏名（名称）を記載し、その次に押印する。

田 辺 恵 基

受理官庁記入欄

1. 国際出願として提出された書類の実際の受理の日

3. 国際出願として提出された書類を補充する書類又は図面であって

その後期間内に提出されたものの実際の受理の日（訂正日）

4. 特許協力条約第11条(2)に基づく必要な補充の期間内の受理の日

5. 出願人により特定された
国際調査機関

ISA / JP

6. ☐ 調査手数料未払いにつき、国際調査機関に
調査用写しを送付していない

2. 図面

☐ 受理された☐ 不足図面がある

国際事務局記入欄

記録原本の受理の日

This Page Blank (uspto)

P C T

手数料計算用紙

願 害 附 属 書

受理官庁記入欄

国際出願番号

出願人又は代理人の書類記号

S 00 P 0777 W O 00

受理官庁の日付印

出願人

ソニー株式会社 SONY CORPORATION

所定の手数料の計算

1. 及び 2. 特許協力条約に基づく国際出願等に関する法律（国内法）
第 18 条第 1 項第 1 号の規定による手数料（注 1）
（送付手数料 [T] 及び調査手数料 [S] の合計）

95,000 円 T + S

3. 国際手数料（注 2）

基本手数料

国際出願に含まれる用紙の枚数 130 枚

最初の 30 枚まで

46,000 円 b 1

100 × 1,100 =

110,000 円 b 2

30 枚を超える用紙の枚数 用紙 1 枚の手数料

b 1 及び b 2 に記入した金額を加算し、合計額を B に記入

156,000 円 B

指定手数料

国際出願に含まれる指定数（注 3） 5

5 × 9,900 =

49,500 円 D

支払うべき指定手数料
の数（上限は 8）
（注 4）
1 指定当たりの手数料

B 及び D に記入した金額を加算し、合計額を I に記入

205,500 円 I

4. 納付すべき手数料の合計

T + S 及び I に記入した金額を加算し、合計額を合計に記入

300,500 円

合 計

（注 1）送付手数料及び調査手数料については、合計金額を特許印紙をもって納付しなければならない。

（注 2）国際手数料については、受理官庁である日本国特許庁の長官が告示する国際事務局の口座への振込みを証明する書面を提出することにより納付しなければならない。

（注 3）願書第 V 欄でレ印を付した口の数。

（注 4）指定数を記入する。ただし、8 指定以上は一律 8 とする。

This Page Blank (uspto)



送付手数料 (18,000円)
調査手数料 (77,000円)

This Page Blank (uspto)

依頼日 000407

振込金(兼消費税等込手数料)受取書

先方銀行 漢字 東京三菱 様

お受取人 カタカナ ワイホロキーニイテ 様

おなまえ WIP0-PCT 様

おところ おでんわ(03) 3506-3856

ご依頼人 カタカナ タナハシケモト 様

おでんわ先 03-3470-6570

おなまえ 田辺東基 様

おところ 渋谷区神宮前1-11-11-508
グリーンファンタジアビル 5F

〇印をおつけください。 振込先 内幸町 様

振込金額 0473286 千円

手数料 735 円

受取人等はカナ文字で送信しますので、フリガナは正しくいぬいにご記入ください。
振込依頼書にご記入相違等の不備があると照会等のため振込が遅延することがあります。
午後2時以降のご用命の場合は、当日中に入金できないこともございますので、あらかじめご了承ください。
万一、通信機器・回線等の障害が生じた場合、振込が遅延したことによる補償はできませんのでご了承ください。

当行をご利用くださいますとありがとうございます。 翌日発信扱
今後ともよろしくお願い申し上げます。

当行本支店への振込のために受入れた下記の小切手等が不渡りとなったときは、その金額の振込を取消し、その小切手等は権利保全の手続きをしないで当店において返却します。

未決済小切手等

株式会社 国民銀行
原宿支店

収入印紙
振込金+手数料
3万円以上貼付
17号文書
(払戻請求書による受付書としたものは非課税)

(為104)

基本手数料 { 156,000円 }
指定手数料 { 49,500円 }
計 205,500 円

This Page Blank (uspto)

控

優先権証明願 (PCT)



特許庁長官 近藤 隆彦 殿

1. 出願番号 平成11年特許願第103992号

2. 請求人

識別番号 100082740

住 所 東京都渋谷区神宮前1丁目11番11-508号
グリーンファンタジアビル5階

氏 名 弁理士 田辺 恵基

電話番号 03-3470-6591

3. 出願国名 PCT



(1,500円)

This Page Blank (uspto)

委任状

私は弁理士 田 辺 恵 基 識別番号 100082740 を代理人と
定めて下記事項を委任する

1. 優先権取得に関する一切の件
(特願平11-103992号)
2. 上記事件につき、出願の分割、出願の変更、放棄若しくは取
下げ、特許権の存続期間の延長登録の出願の取下げ、請求、
申請若しくは申立ての取下げ、特許法第41条第1項若しく
は実用新案法第8条第1項の優先権の主張若しくはその取下
げ、拒絶査定に対する審判の請求、実用新案登録出願若しく
は実用新案登録についての実用新案技術評価の請求、又は復
代理人の選任若しくは解任をするの件

以上

平成 12 年 4 月 / 日

東京都品川区北品川6丁目7番35号

ソニー株式会社

代表取締役 出井伸之



This Page Blank (uspto)

PCT

国際調査報告

(法 8 条、法施行規則第40、41条)
[PCT 18 条、PCT 規則43、44]

出願人又は代理人 の書類記号 S00P0777WO00	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220) 及び下記 5 を参照すること。	
国際出願番号 PCT/JPO0/02290	国際出願日 (日.月.年) 07.04.00	優先日 (日.月.年) 12.04.99
出願人 (氏名又は名称) ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条 (PCT 18 条) の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 2 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない (第 I 欄参照)。

3. ☐ 発明の単一性が欠如している (第 II 欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。

☐ 第 III 欄に示されているように、法施行規則第47条 (PCT 規則38.2(b)) の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から 1 カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 13 図とする。 ☒ 出願人が示したとおりである。

☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

This Page Blank (uspto)

A 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F17/60

調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F17/60 G06F13/00 G09C1/00 H04L9/08 G06F15/00 H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年

日本国公開実用新案公報 1971-2000年

日本国実用新案登録公報 1996-2000年

日本国登録実用新案公報 1994-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル(JOIS)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	WO, 96/27155, A2 (InerTrust Technologies Corp.) 6.9月.1996 (06.09.96) & JP, 10-512074, A	1-8
Y	人文科学とコンピュータ, 第36-8巻, 11月.1997 河原正治「著作権処理技術の最近の動向」 p. 43-48	1-8

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

24.05.00

国際調査報告の発送日

13.06.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

岩間 直純



5L

9287

電話番号 03-3581-1101 内線 3562

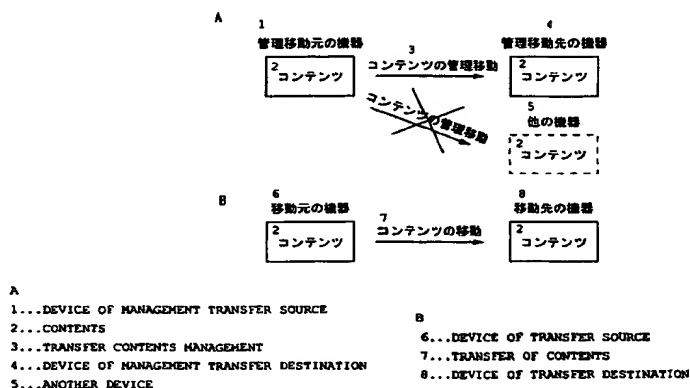
This Page Blank (uspto)



(51) 国際特許分類7 G06F 17/60	A1	(11) 国際公開番号 WO00/62217 (43) 国際公開日 2000年10月19日(19.10.00)
(21) 国際出願番号 PCT/JP00/02290 (22) 国際出願日 2000年4月7日(07.04.00) (30) 優先権データ 特願平11/103992 1999年4月12日(12.04.99) JP (71) 出願人 (米国を除くすべての指定国について) ソニー株式会社(SONY CORPORATION)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP) (72) 発明者 ; および (75) 発明者 / 出願人 (米国についてののみ) 石橋義人(ISHIBASHI, Yoshihito)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo, (JP) (74) 代理人 弁理士 田辺恵基(TANABE, Shigemoto) 〒150-0001 東京都渋谷区神宮前1丁目11番11-508号 グリーンフアンタジアビル5階 Tokyo, (JP)	(81) 指定国 CN, KR, SG, US, 欧州特許 (DE, FR, GB) 添付公開書類 国際調査報告書	

(54) Title: INFORMATION PROCESSING DEVICE AND METHOD, AND PROVIDING MEDIUM

(54) 発明の名称 情報処理装置および方法、並びに提供媒体



(57) Abstract

Contents can be transferred while the device which is the source of the contents holds them. The contents are transferred to a device of a management transfer destination while being held in the device of the management transfer source. The contents are used by both the device of the management transfer source and the device of the management transfer destination. This is different from ordinary transfer that the contents are not held in the device of the transfer source but used exclusively by the device of the transfer destination. During the management transfer of the contents, the device of the management transfer source cannot transfer the management of the contents to another device. The contents are held exclusively in the two devices, the device of the management transfer source and the device of the management transfer destination. This is different from duplication of the first generation that a plurality of duplicates (of the first generation) can be created from the original contents. This is also different from the one-time duplication because the management of the contents can be transferred to another device by returning them from the device of the management transfer source.

(57)要約

コンテンツの移動元の機器が、コンテンツを保持しつつ、コンテンツを移動させることができるようにする。

管理移動元の機器にコンテンツが保持されつつ、管理移動先の機器にそのコンテンツが移動される。管理移動元の機器と管理移動先の機器の両方において、コンテンツが利用される。つまり、移動元の機器にコンテンツが保持されず、移動先の機器においてのみコンテンツが利用される、通常の移動とは異なる。コンテンツの管理移動が行われている間、管理移動元の機器は、他の機器にコンテンツを管理移動することができない。管理移動元の機器と管理移動先の機器の2機においてのみコンテンツが保持される。つまり、オリジナルのコンテンツから、複数の複製（第1世代）を作成することができる、第1世代の複製とも異なる。管理移動元の機器からコンテンツを戻すことより、他の機器にコンテンツを管理移動することができるので、1回だけの複製とも異なる。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AG	アンティグア・バーブーダ	DZ	アルジェリア	LC	セントルシア	SD	スーダン
AL	アルバニア	EE	エストニア	LI	リヒテンシュタイン	SE	スウェーデン
AM	アルメニア	ES	スペイン	LK	スリ・ランカ	SG	シンガポール
AT	オーストリア	FI	フィンランド	LR	リベリア	SI	スロヴェニア
AU	オーストラリア	FR	フランス	LS	レソト	SK	スロヴァキア
AZ	アゼルバイジャン	GA	ガボン	LT	リトアニア	SL	シエラ・レオネ
BA	ボスニア・ヘルツェゴビナ	GB	英国	LU	ルクセンブルグ	SN	セネガル
BB	バルバドス	GD	グレナダ	LV	ラトヴィア	SZ	スワジランド
BE	ベルギー	GE	グルジア	MA	モロッコ	TD	チャード
BF	ブルキナ・ファソ	GH	ガーナ	MC	モナコ	TG	トーゴ
BG	ブルガリア	GM	ガンビア	MD	モルドヴァ	TJ	タジキスタン
BJ	ベナン	GN	ギニア	MG	マダガスカル	TM	トルクメニスタン
BR	ブラジル	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア	TR	トルコ
BY	ベラルーシ	GW	ギニア・ビサウ		共和国	TT	トリニダード・トバゴ
CA	カナダ	HR	クロアチア	ML	マリ	TZ	タンザニア
CF	中央アフリカ	HU	ハンガリー	MN	モンゴル	UA	ウクライナ
CG	コンゴ	ID	インドネシア	MR	モリタニア	UG	ウガンダ
CH	スイス	IE	アイルランド	MW	マラウイ	US	米国
CI	コートジボアール	IL	イスラエル	MX	メキシコ	UZ	ウズベキスタン
CM	カメルーン	IN	インド	MZ	モザンビーク	VN	ヴェトナム
CN	中国	IS	アイスランド	NE	ニジェール	YU	ユーゴスラヴィア
CR	コスタ・リカ	IT	イタリア	NL	オランダ	ZA	南アフリカ共和国
CU	キューバ			NO	ノルウェー	ZW	ジンバブエ
CY	キプロス	JP	日本	NZ	ニュージーランド		
DE	チェッコ	KE	ケニア	PL	ポーランド		
DK	デンマーク	KG	キルギスタン	PT	ポルトガル		
		KP	北朝鮮	RO	ルーマニア		
		KR	韓国				

明 細 書

情報処理装置および方法、並びに提供媒体

技術分野

本発明は、情報処理装置および方法、並びに提供媒体に関し、特に、暗号化された情報を利用する情報処理装置および方法、並びに提供媒体に関する。

背景技術

音楽などの情報（以下、コンテンツと称する）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザが、情報処理装置でコンテンツを復号して、利用するシステムがある。

また、コンテンツを利用することができる情報処理装置が複数存在する場合、ユーザは、提供されてコンテンツを移動させ、コンテンツが移動された情報処理装置において、コンテンツを利用することもできる。

しかしながら、この場合、コンテンツは移動元の情報処理装置が保持されず、ユーザが、移動元の情報処理装置において、そのコンテンツを利用できない課題があった。

発明の開示

本発明はこのような状況に鑑みてなされたものであり、コンテンツが移動元の情報処理装置にも保持され、他の情報処理装置にコンテンツを移動させることができるようにするものである。

かかる課題を解決するため本発明においては、情報処理装置において、他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置において、価値情報を復号するのに必要な鍵、価値情報の使用条件、および価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する

記憶手段と、記憶手段により記憶されている利用情報に含まれる前記使用条件が所定の条件で、かつ、利用情報に含まれる移動状態情報が、価値情報の移動が行われていないことを示しているとき、価値情報、および利用情報に含まれる鍵を含む所定の移動情報を他の情報処理装置に供給する供給手段と、供給手段により、価値情報、および移動情報が他の情報処理装置に供給されたとき、移動状態情報の内容を、価値情報の移動が行われていることを示すものに変更する第1の変更手段と、記憶手段により記憶されている利用情報に含まれる移動状態情報が、価値情報の移動が行われていることを示しており、情報処理装置への価値情報の移動を解除するとき、他の情報処理装置に所定の制御信号を送信する送信手段と、他の情報処理装置から、送信手段により送信された制御信号に対する応答信号を受信したとき、移動状態情報の内容を、価値情報の移動が行われていないことを示すものに変更する第2の変更手段とを具備する。

また本発明においては、情報処理方法において、他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置の情報処理方法において、価値情報を復号するのに必要な鍵、価値情報の使用条件、および価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶ステップと、記憶ステップで記憶された利用情報に含まれる使用条件が所定の条件で、かつ、利用情報に含まれる移動状態情報が、価値情報の移動が行われていないことを示しているとき、価値情報、および利用情報に含まれる鍵を含む所定の移動情報を他の情報処理装置に供給する供給ステップと、供給ステップで、価値情報、および移動情報が他の情報処理装置に供給されたとき、移動状態情報の内容を、価値情報の移動が行われていることを示すものに変更する第1の変更ステップと、記憶ステップで記憶されている利用情報に含まれる移動状態情報が、価値情報の移動が行われていることを示しており、情報処理装置への価値情報の移動を解除するとき、他の情報処理装置に所定の制御信号を送信する送信ステップと、他の情報処理装置から、送信ステップで送信された制御信号に対する応答信号を受信したとき、移動状態情報の内容を、価値情報の移動が行われていないこ

とを示すものに変更する第2の変更ステップを具備する。

さらに本発明においては、提供媒体において、他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置に、価値情報を復号するのに必要な鍵、価値情報の使用条件、および価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶ステップと、記憶ステップで記憶された利用情報に含まれる使用条件が所定の条件で、かつ、利用情報に含まれる移動状態情報が、価値情報の移動が行われていないことを示しているとき、価値情報、および利用情報に含まれる鍵を含む所定の移動情報を他の情報処理装置に供給する供給ステップと、供給ステップで、価値情報、および移動情報が他の情報処理装置に供給されたとき、移動状態情報の内容を、価値情報の移動が行われていることを示すものに変更する第1の変更ステップと、記憶ステップで記憶されている利用情報に含まれる移動状態情報が、価値情報の移動が行われていることを示しており、他の情報処理装置への価値情報の移動を解除するとき、他の情報処理装置に所定の制御信号を送信する送信ステップと、他の情報処理装置から、送信ステップで送信された制御信号に対する応答信号を受信したとき、移動状態情報の内容を、価値情報の移動が行われていないことを示すものに変更する第2の変更ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供。

さらに本発明においては、情報処理装置、情報処理方法、および提供媒体において、価値情報を復号するのに必要な鍵、価値情報の使用条件、および価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報が記憶され、記憶された利用情報に含まれる使用条件が所定の条件で、かつ、利用情報に含まれる移動状態情報が、価値情報の移動が行われていないことを示しているとき、価値情報、および利用情報に含まれる鍵を含む所定の移動情報が他の情報処理装置に供給され、価値情報、および移動情報が他の情報処理装置に供給されたとき、移動状態情報の内容が、価値情報の移動が行われていることを示すものに変更され、記憶されている利用情報に含まれる移動状態情報が、価値情報の移動が行わ

れていることを示しており、他の情報処理装置への価値情報の移動を解除するとき、他の情報処理装置に所定の制御信号が送信され、他の情報処理装置から、制御信号に対する応答信号が受信されたとき、移動状態情報の内容が、価値情報の移動が行われていないことを示すものに変更される。

さらに本発明においては、情報処理装置において、他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置において、他の情報処理装置から供給される価値情報、および価値情報を復号するのに必要な鍵を含む移動情報を受信する受信手段と、受信手段により受信された移動情報を記憶する記憶手段と、他の情報処理装置から、所定の制御信号を受信したとき、記憶手段に記憶されている移動情報を削除する削除手段と、削除手段により、移動情報が削除されたとき、所定の応答信号を送信する送信手段を具備する。

さらに本発明においては、情報処理方法において、他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置の情報処理方法において、他の情報処理装置から供給される価値情報、および価値情報を復号するのに必要な鍵を含む移動情報を受信する受信ステップと、受信ステップで受信された移動情報を記憶する記憶ステップと、他の情報処理装置から、所定の制御信号を受信したとき、記憶ステップで記憶された移動情報を削除する削除ステップと、削除ステップで、移動情報が削除されたとき、所定の応答信号を送信する送信ステップを具備する。

さらに本発明においては、提供媒体において、他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置に、他の情報処理装置から供給される価値情報、および価値情報を復号するのに必要な鍵を含む移動情報を受信する受信ステップと、受信ステップで受信された移動情報を記憶する記憶ステップと、他の情報処理装置から、所定の制御信号を受信したとき、記憶ステップで記憶された移動情報を削除する削除ステップと、削除ステップで、移動情報が削除されたとき、所定の応答信号を送信する送信ステップとを具備する処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴と

する。

さらに本発明においては、情報処理装置、情報処理方法、および提供媒体において、他の情報処理装置から供給される価値情報、および価値情報を復号するのに必要な鍵を含む移動情報が受信され、受信された価値情報が記憶され、他の情報処理装置から、所定の制御信号を受信したとき、記憶された移動情報が削除され、移動情報が削除されたとき、所定の応答信号が送信される。

図面の簡単な説明

図 1 は、EMD システムを説明する系統図である。

図 2 は、EMD システムにおける、主な情報の流れを説明する系統図である。

図 3 は、EMD サービスセンタ 1 の機能的構成を示すブロック図である。

図 4 は、EMD サービスセンタ 1 の配送用鍵 K d の送信を説明する略線図である。

図 5 は、EMD サービスセンタ 1 の配送用鍵 K d の送信を説明する他の略線図である。

図 6 は、EMD サービスセンタ 1 の配送用鍵 K d の送信を説明する他の略線図である。

図 7 は、EMD サービスセンタ 1 の配送用鍵 K d の送信を説明する他の略線図である。

図 8 は、EMD サービスセンタ 1 の配送用鍵 K d の送信を説明する他の図表である。

図 9 は、システム登録情報を説明する図表である。

図 10 は、利用ポイント情報を説明する図表である。

図 11 は、コンテンツプロバイダ 2 の機能的構成例を示すブロック図である。

図 12 は、UCP を説明する図表である。

図 13 は、コンテンツの管理移動を説明する略線図である。

図 14 は、第 1 世代複製を説明する略線図である。

図 1 5 は、サービスコードおよびコンディションコードのコード値の例を示す図表である。

図 1 6 は、U C P の利用条件として設定されたコード値の例を示す図表である。

図 1 7 は、コンテンツプロバイダセキュアコンテナの例を示す略線図である。

図 1 8 は、コンテンツプロバイダ 2 の証明書の例を示す略線図である。

図 1 9 は、サービスプロバイダ 3 の機能の構成を示すブロック図である。

図 2 0 は、P T の例を示す図表である。

図 2 1 は、P T の価格条件として設定されたコード値の例を示す図表である。

図 2 2 は、他の P T の例を示す図表である。

図 2 3 は、他の P T の価格条件として設定されたコード値の例を示す図表である。

図 2 4 は、サービスプロバイダセキュアコンテナの例を示す略線図である。

図 2 5 は、サービスプロバイダ 3 の証明書の例を示す略線図である。

図 2 6 は、ユーザホームネットワーク 5 のレシーバ 5 1 の機能的構成例を示すブロック図である。

図 2 7 は、レシーバ 5 1 の S A M 6 2 の証明書の例を示す略線図である。

図 2 8 は、U C S の例を示す図表である。

図 2 9 は、レシーバ 5 1 の外部記憶部 6 3 の利用情報記憶部 6 3 A の内部を説明する略線図である。

図 3 0 は、課金情報の例を示す図表である。

図 3 1 は、レシーバ 5 1 の記憶モジュール 7 3 に記憶されている情報を示す図表である。

図 3 2 は、基準情報 5 1 を説明する図表である。

図 3 3 は、基準情報 5 1 の利用ポイント情報の例を示す図表である。

図 3 4 は、登録リストの例を示す図表である。

図 3 5 は、ユーザホームネットワーク 5 のレシーバ 2 0 1 の機能的構成例を示

すブロック図である。

図36は、レシーバ201の外部記憶部213の移動情報記憶部213Aの内部を説明する略線図である。

図37は、レシーバ201の記憶モジュール223に記憶されている情報を示す図表である。

図38は、コンテンツの利用処理を説明するフローチャートである。

図39は、EMDサービスセンタ1がコンテンツプロバイダ2へ配送用鍵Kdを送信する処理を説明するフローチャートである。

図40は、コンテンツプロバイダ2とEMDサービスセンタ1との相互認証の動作を説明するフローチャートである。

図41は、コンテンツプロバイダ2とEMDサービスセンタ1との相互認証の他の動作を説明するフローチャートである。

図42は、コンテンツプロバイダ2とEMDサービスセンタ1との相互認証の他の動作を説明するフローチャートである。

図43は、コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

図44は、サービスプロバイダ3がレシーバ51にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

図45は、レシーバ51がサービスプロバイダセキュアコンテナを受信する処理を説明するフローチャートである。

図46は、レシーバ51がコンテンツを再生する処理を説明するフローチャートである。

図47は、課金を決済する処理を説明するフローチャートである。

図48は、コンテンツを管理移動する処理を説明するフローチャートである。

図49は、コンテンツの管理移動を終了する処理を説明するフローチャートである。

発明を実施するための最良の形態

以下に本発明の実施の形態を説明する。

(1) 情報配信システム

図1は、本発明を適用したEMD (Electronic Music Distribution: 電子音楽配信) システムを説明する図である。EMDシステムは、各装置を管理するEMDサービスセンタ1、コンテンツを提供するコンテンツプロバイダ2 (この例の場合、2つのコンテンツプロバイダ2-1, 2-2 (以下、個々に区別する必要がない場合、単に、コンテンツプロバイダ2と記述する。他の装置についても同様である) が設けられている)、コンテンツに対応するサービスを提供するサービスプロバイダ3 (この例の場合、2つのサービスプロバイダ3-1, 3-2が設けられている)、およびコンテンツが利用されるユーザネットワーク5から構成されている。

EMDシステムにおけるコンテンツ (Content) とは、情報そのものが価値を有するデジタルデータで、この例の場合、1つのコンテンツは、1曲分の音楽データに相当する。またコンテンツは、1つのコンテンツを1つの単位 (シングル) として、または複数のコンテンツを1つの単位 (アルバム) としてユーザに提供される。ユーザは、コンテンツを購入し (実際は、コンテンツを利用する権利を購入し)、コンテンツを利用する。尚、コンテンツは、音楽データだけでなく、映像データ、ゲームプログラム、コンピュータプログラム、著作データなどの場合も有りうる。

EMDサービスセンタ1は、EMDシステムにおける主な情報の流れを示す図2に示すように、ユーザホームネットワーク5、およびコンテンツプロバイダ2に、コンテンツを利用するために必要な配送用鍵K_dを送信する。EMDサービスセンタ1はまた、ユーザホームネットワーク5の機器から、課金情報等を受信して、料金を精算する処理などを実行する。

コンテンツプロバイダ2-1, 2-2は、図2に示すように、提供するコンテンツ (コンテンツ鍵K_{co}で暗号化されている)、そのコンテンツを復号するた

めに必要なコンテンツ鍵K c o（配送用鍵K dで暗号化されている）、およびコンテンツの利用内容などを示す取扱方針（以下、UCP（U s a g e C o n t r o l P o l i c y）と記述する）を保持し、それらを、コンテンツプロバイダセキュアコンテナ（後述）と称する形態で、サービスプロバイダ3に供給する。

サービスプロバイダ3-1, 3-2は、コンテンツプロバイダ2から供給されるUCPに対応して、1つまたは複数の価格情報（以下、PT（P r i c e T a g）と記述する）を作成し、それを保持する。サービスプロバイダ2は、作成したPTを、コンテンツプロバイダ2から供給されたコンテンツ（コンテンツ鍵K c oで暗号化されている）、コンテンツ鍵K c o（配送用鍵K dで暗号化されている）、およびUCPとともに、サービスプロバイダセキュアコンテナと称する形態で、専用のケーブルネットワーク、インターネット、または衛星通信などから構成されるネットワーク4を介して、ユーザホームネットワーク5に送信する。

ユーザホームネットワーク5は、供給されたUCPおよびPTに基づいて、図2に示すように、使用許諾条件情報（以下、UCS（U s a g e C o n t r o l S t a t u s）と称する）を作成し、作成したUCSに基づいてコンテンツを利用する処理を実行する。ユーザホームネットワーク5はまた、UCSを作成するタイミングで課金情報を作成し、例えば、配送用鍵K dの供給を受けのタイミングで、対応するUCPおよびPTなどとともにEMDサービスセンタ1に送信する。なお、ユーザホームネットワーク5は、UCPおよびPTをEMDサービスセンタ1に送信しないようにすることもできる。

この例の場合、ユーザホームネットワーク5は、HDD52に接続され、SAM（S e c u r e A p p l i c a t i o n M o d u l e）62を有するレシーバ51、およびHDD202に接続され、SAM212を有するレシーバ201から構成されている。レシーバ51とレシーバ201は、IEEE1394等で接続されている。

(2) EMDサービスセンタ

図3は、EMDサービスセンタ1の機能的構成を示すブロック図である。サービスプロバイダ管理部11は、サービスプロバイダ3に利益分配の情報を供給する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2に配送用鍵Kdを送信したり、利益分配の情報を供給する。

著作権管理部13は、ユーザホームネットワーク5のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC (Japanese Society for Rights of Authors, Composers and Publishers: 日本音楽著作権協会) に送信する。

鍵サーバ14は、配送用鍵Kdを記憶しており、それを、コンテンツプロバイダ管理部12を介してコンテンツプロバイダ2に供給したり、ユーザ管理部18等を介してユーザホームネットワーク5に供給する。

ユーザホームネットワーク5の機器(例えば、レシーバ51またはレシーバ201)およびコンテンツプロバイダ2に供給される、EMDサービスセンタ1からの配送用鍵Kdについて、図4乃至図7を参照して説明する。

図4は、コンテンツプロバイダ2がコンテンツの提供を開始し、ユーザホームネットワーク5を構成するレシーバ51がコンテンツの利用を開始する、1998年1月における、EMDサービスセンタ1が有する配送用鍵Kd、コンテンツプロバイダ2が有する配送用鍵Kd、およびレシーバ51が有する配送用鍵Kdを示す図である。

図4の例において、配送用鍵Kdは、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である” a a a a a a a a ”の値を有するバージョン1である配送用鍵Kdは、1998年1月1日から1998年1月31日まで使用可能(すなわち、1998年1月1日から1998年1月31日の期間にサービスプロバイダ3を介してユーザホームネットワーク5に配布されるコンテンツを暗号化するコンテンツ鍵Kc oは、バージョン1である配送

用鍵K dで暗号化されている)であり、所定のビット数の乱数である” b b b b b b b b” の値を有するバージョン2である配送用鍵K dは、1998年2月1日から1998年2月28日まで使用可能(すなわち、その期間にサービスプロバイダ3を介してユーザホームネットワーク5に配布されるコンテンツを暗号化するコンテンツ鍵K c oは、バージョン2である配送用鍵K dで暗号化されている)である。同様に、バージョン3である配送用鍵K dは、1998年3月中に使用可能であり、バージョン4である配送用鍵K dは、1998年4月中に使用可能であり、バージョン5である配送用鍵K dは、1998年5月中に使用可能であり、バージョン6である配送用鍵K dは、1998年6月中に使用可能である。

コンテンツプロバイダ2がコンテンツの提供を開始するに先立ち、EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年1月から1998年6月まで利用可能な、バージョン1乃至バージョン6の6つの配送用鍵K dを送信し、コンテンツプロバイダ2は、6つの配送用鍵K dを受信し、記憶する。6ヶ月分の配送用鍵K dを記憶するのは、コンテンツプロバイダ2が、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

また、レシーバ51がコンテンツの利用を開始するに先立ち、EMDサービスセンタ1は、レシーバ51に、1998年1月から1998年3月まで、利用可能なバージョン1乃至バージョン3である3つの配送用鍵K dを送信し、レシーバ51は、3つの配送用鍵K dを受信し、記憶する。3ヶ月分の配送用鍵K dを記憶するのは、レシーバ51が、EMDサービスセンタ1に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ1への接続の頻度を低くし、ユーザホームネットワーク5の負荷を低減するためである。

1998年1月1日から1998年1月31日の期間には、バージョン1であ

る配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

1998年2月1日における、EMDサービスセンタ1の配送用鍵K dのコンテンツプロバイダ2、およびレシーバ51への送信を図5で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年2月から1998年7月まで利用可能な、バージョン2乃至バージョン7の6つの配送用鍵K dを送信し、コンテンツプロバイダ2は、6つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年2月から1998年4月まで、利用可能なバージョン2乃至バージョン4である3つの配送用鍵K dを送信し、レシーバ51は、3つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵K dをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵K dを利用できるようにするためである。

1998年2月1日から1998年2月28日の期間には、バージョン2である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

1998年3月1日における、EMDサービスセンタ1の配送用鍵K dのコンテンツプロバイダ2、およびレシーバ51への送信を図6で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年3月から1998年8月まで利用可能な、バージョン3乃至バージョン8の6つの配送用鍵K dを送信し、コンテンツプロバイダ2は、6つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年3月から1998年5月まで、利用可能なバージョン3乃至バージョン5である3つの配送用鍵K dを送信し、レシーバ51は、3つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K

dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵K dおよびバージョン2である配送用鍵K dをそのまま記憶する。

1998年3月1日から1998年3月31日の期間には、バージョン3である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

1998年4月1日における、EMDサービスセンタ1の配送用鍵K dのコンテンツプロバイダ2、およびレシーバ51への送信を図7で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年4月から1998年9月まで利用可能な、バージョン4乃至バージョン9の6つの配送用鍵K dを送信し、コンテンツプロバイダ2は、6つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年4月から1998年6月まで、利用可能なバージョン3乃至バージョン5である3つの配送用鍵K dを送信し、レシーバ51は、3つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵K d、バージョン2である配送用鍵K d、およびバージョン3である配送用鍵K dをそのまま記憶する。

1998年4月1日から1998年4月30日の期間には、バージョン4である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

このように、あらかじめ先の月の配送用鍵K dを配布しておくことで、仮にユーザが1, 2ヶ月まったくEMDサービスセンタ1にアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、EMDサービスセンタ1にアクセスして鍵を受信することができる。

ユーザホームネットワーク5の、EMDシステムに正式登録された機器、およびコンテンツプロバイダ2には、以上のように、3ヶ月分の配送用鍵K dが配布

されるが、EMDシステムに正式登録されておらず、仮登録（詳細は後述する）されている状態の、ユーザホームネットワーク 5 の機器には、3 ヶ月分の配送用鍵 K d に代わり、図 8 に示すような、1 ヶ月分の配送用鍵 K d が配布される。この例においては、ユーザホームネットワーク 5 の機器を EMD システムに正式登録するために、与信処理など、約 1 ヶ月程度の時間を有する登録手続が必要となる。そこで、登録申請から正式登録されるまでの間（約 1 ヶ月間）においても、コンテンツの利用が可能となるように、正式登録されていない機器（仮登録されている機器）には、1 ヶ月間において利用可能な配送用鍵 K d が配布される。

図 3 に戻り、経歴データ管理部 1 5 は、ユーザ管理部 1 8 から出力される、課金情報、そのコンテンツに対応する P T、およびそのコンテンツに対応する U C P などを記憶する。

利益分配部 1 6 は、経歴データ管理部 1 5 から供給された各種情報に基づき、EMD サービスセンタ 1、コンテンツプロバイダ 2-1、2-2、およびサービスプロバイダ 3-1、3-2 の利益をそれぞれ算出し、その結果をサービスプロバイダ管理部 1 1、コンテンツプロバイダ管理部 1 2、出納部 2 0、および著作権管理部 1 3 に出力する。利益配分部 1 6 はまた、算出した利益に応じてコンテンツプロバイダ 2-1、2-2 およびサービスプロバイダ 3-1、3-2 のそれぞれに対する利用ポイント（利益が大きければ大きいほど、すなわち、ユーザが利用すればするほど、大きい値となるポイント）を算出し、ユーザ管理部 1 8 に出力する。なお、以下において、コンテンツプロバイダ 2 における利用ポイントをコンテンツ利用ポイントと称し、サービスプロバイダ 3 における利用ポイントをサービス利用ポイントと称する。

相互認証部 1 7 は、コンテンツプロバイダ 2、サービスプロバイダ 3、およびユーザホームネットワーク 5 の機器と相互認証を実行する。

ユーザ管理部 1 8 は、ユーザホームネットワーク 5 の機器に関する情報（以下、システム登録情報と称する）を管理する。システム登録情報には、図 9 に示すように、「SAM の I D」、「機器番号」、「決済 I D」、「決済ユーザ情報」

、複数の「従属ユーザ情報」、および「利用ポイント情報」の項目に対応する所定の情報が含まれている。

「SAMのID」には、製造された、ユーザホームネットワーク5の機器のSAMのIDが記憶される。図9のシステム登録情報の「SAMのID」には、レシーバ51のSAM62のIDおよびレシーバ201のSAM212のIDが設定されている。

「機器番号」には、SAMを有するユーザホームネットワーク5の機器に、予め設定された機器番号が設定されている。ユーザホームネットワーク5の機器が、ネットワーク4を介してサービスプロバイダ3と、およびEMDサービスセンタ1と直接通信することができる機能を有し（通信部を有し）、かつ、例えば、UCPやPTの内容をユーザに出力（提示）したり、ユーザがUCPの利用内容を選択することができる機能を有している（表示部および操作部を有している）場合、その機器（以下、主機器と称する）には、100番以上の機器番号が与えられる。機器が、そのような機能を有しない場合、その機器（以下、従機器と称する）には、99番以下の機器番号が与えられる。この例の場合、詳細は後述するが、レシーバ51およびレシーバ201の両者は、上述した機能を有しているので、それぞれには、100番以上の機器番号（100番）が与えられてる。そこで、図9のシステム登録情報の「機器番号」には、レシーバ51のSAM62のIDおよびレシーバ201のSAM212のIDに対応する「機器番号」のそれぞれには、機器番号100番が設定されている。

「決済ID」には、EMDシステムに正式登録されたとき割り当てられる所定の決済IDが記憶される。この例の場合、レシーバ51およびレシーバ201は共に、正式登録され、決済IDが与えられているので、図9のシステム登録情報の、SAM62のIDおよびSAM212のIDに対応する「決済ID」のそれぞれには、その与えられた決済IDが記憶されている。

「決済ユーザ情報」には、計上される課金を決済するユーザ（以下、このようなユーザを決済ユーザと称する）の、氏名、住所、電話番号、決済機関情報（例

えば、クレジットカード番号等)、生年月日、年齢、性別、ID、パスワードなどが設定される。

「決済ユーザ情報」に設定される決済ユーザの、氏名、住所、電話番号、決済機関の情報、生年月日、および性別(以下、ここに区別する必要がない場合、これらの情報をまとめて、ユーザ一般情報と称する)は、登録が申請される際にユーザから提供され、設定されるが、この例の場合、そのうち、氏名、住所、電話番号、および決済機関の情報は、それらに基づいて与信処理が行われるので、正確な情報(例えば、決済機関に登録されている情報)である必要がある。それに対して、ユーザ一般情報の生年月日、年齢、および性別は、与信処理には用いられないので、この例の場合、それらの情報は、正確である必要はなく、またユーザは、その情報を必ずしも提供する必要がない。「決済ユーザ情報」に記憶される決済ユーザの、IDおよびパスワードは、EMDシステムに仮登録されるときに割り当てられ、設定される。

図9のシステム登録情報には、レシーバ51のSAM62のIDに対応する「決済ユーザ情報」には、レシーバ51の決済ユーザである、ユーザFの、ユーザ一般情報、ID、およびパスワードが設定され、レシーバ201のSAM212のIDに対応する「決済ユーザ情報」には、レシーバ201の決済ユーザである、ユーザAの、ユーザ一般情報、ID、およびパスワードが設定されている。

「従属ユーザ情報」には、課金を決済しないユーザ(以下、このようなユーザを従属ユーザと称する)の、氏名、住所、電話番号、生年月日、年齢、性別、ID、パスワードなどが設定される。すなわち、「決済ユーザ情報」に設定される情報のうち、決済機関の情報以外の情報が設定される。従属ユーザに対しては与信処理が行われないので、「従属ユーザ情報」に設定される従属ユーザの、氏名、住所、電話番号、生年月日、年齢、および性別の情報は、正確なものである必要がない。例えば、氏名の場合は、ニックネームのようなものでもよい。また氏名はユーザを特定するために必要とされるが、他の情報は、ユーザは必ずしも提供する必要がない。「従属ユーザ情報」に設定される従属ユーザの、IDおよび

パスワードは、仮登録または正式登録されるときに割り当てられ、設定される。

この例の場合、レシーバ51およびレシーバ201の両者には、従属ユーザが登録されていないので、図9のシステム登録情報のSAM62のIDに対応する「従属ユーザ情報」、およびSAM212のIDに対応する「従属ユーザ情報」には、何の情報も設定されていない。

「利用ポイント情報」には、利益分配部16から出力された利用ポイントが設定される。この例の場合、SAM62およびSAM212に対応する「利用ポイント情報」には、それぞれの利用ポイント情報が設定されている。図10は、レシーバ51の利用ポイント情報の例を示している。図10の例では、レシーバ51のユーザF（決済ユーザ）に与えられている、コンテンツプロバイダ2-1のコンテンツ利用ポイントが222ポイントで、コンテンツプロバイダ2-2のコンテンツ利用ポイントが123ポイントで、サービスプロバイダ3-1のサービス利用ポイントが、345ポイントで、そして、サービスプロバイダ3-2のサービス利用ポイントが0ポイントであるとされている。

なお、この例において、コンテンツプロバイダ2-1およびコンテンツプロバイダ2-2のそれぞれのコンテンツ利用ポイントの合計ポイント345（ $=123+222$ ）と、サービスプロバイダ3-1およびサービスプロバイダ3-2のそれぞれのサービス利用ポイントの合計ポイント345（ $=345+0$ ）が等しくなるようになされている。

レシーバ201においては、現時点でコンテンツは利用されていないので、SAM212のIDに対応する「利用ポイント情報」には、何の情報の設定されていない。

ユーザ管理部18は、このようなシステム登録情報を管理する他、所定の処理に対応して登録リスト（後述）を作成し、配送用鍵Kdとともにユーザホームネットワーク5に送信する。

図3に、再度戻り、課金請求部19は、経歴データ管理部15から供給された、例えば、課金情報、UCP、およびPTに基づき、ユーザへの課金を算出し、

その結果を、出納部 20 に供給する。出納部 20 は、ユーザ、コンテンツプロバイダ 2、およびサービスプロバイダ 3 への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。出納部 20 はまた、決算処理の結果をユーザ管理部 18 に通知する。

監査部 21 は、ユーザホームネットワーク 5 の機器から供給された課金情報、PT、および UCP の正当性（すなわち、不正をしていないか）を監査する。なお、この場合、監査部 21 は、コンテンツプロバイダ 2 からの UCP を、サービスプロバイダ 3 からの PT を、そしてユーザホームネットワーク 5 からの、対応する UCP および PT を受け取る。

(3) コンテンツプロバイダ

図 11 は、コンテンツプロバイダ 2-1 の機能的構成を示すブロック図である。コンテンツサーバ 31 は、ユーザに供給するコンテンツを記憶し、ウォーターマーク付加部 32 に供給する。ウォーターマーク付加部 32 は、コンテンツサーバ 31 から供給されたコンテンツにウォーターマーク（電子透かし）を付加し、圧縮部 33 に供給する。

圧縮部 33 は、ウォーターマーク付加部 32 から供給されたコンテンツを、A T R A C 2 (A d a p t i v e T r a n s f o r m A c o u s t i c C o d i n g 2) (商標) 等の方式で圧縮し、暗号化部 34 に供給する。暗号化部 34 は、圧縮部 33 で圧縮されたコンテンツを、乱数発生部 35 から供給された乱数を鍵（以下、この乱数をコンテンツ鍵 K c o と称する）として、D E S (D a t a E n c r y p t i o n S t a n d a r d) などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

乱数発生部 35 は、コンテンツ鍵 K c o となる所定のビット数の乱数を暗号化部 34 および暗号化部 36 に供給する。暗号化部 36 は、コンテンツ鍵 K c o を E M D サービスセンタ 1 から供給された配送用鍵 K d を使用して、D E S などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

DESは、56ビットの共通鍵を用い、平文の64ビットを1ブロックとして処理する暗号方式である。DESの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DESのすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

まず、平文の64ビットは、上位32ビットの H_0 、および下位32ビットの L_0 に分割される。鍵処理部から供給された48ビットの拡大鍵 K_1 、および下位32ビットの L_0 を入力とし、下位32ビットの L_0 を攪拌したF関数の出力が算出される。F関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の2種類の基本変換から構成されている。次に、上位32ビットの H_0 と、F関数の出力が排他的論理和され、その結果は L_1 とされる。 L_0 は、 H_1 とされる。

上位32ビットの H_0 および下位32ビットの L_0 を基に、以上の処理を16回繰り返し、得られた上位32ビットの H_{16} および下位32ビットの L_{16} が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

ポリシー記憶部37は、コンテンツに対応して設定されるUCPを記憶し、セキュアコンテナ作成部38に出力する。図12は、コンテンツサーバ31に保持されているコンテンツAに対応して設定され、ポリシー記憶部37に記憶されているUCPA、Bを表している。UCPは、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「利用条件」、「利用内容」の各項目に対応する所定の情報が含まれる。「コンテンツのID」には、UCPが対応するコンテンツのIDが設定される。UCPA（図12A）およびUCPB（図12B）のそれぞれの「コンテンツのID」には、コンテンツAのIDが設定されている。

「コンテンツプロバイダのID」には、コンテンツの提供元のコンテンツプロバイダのIDが設定される。UCPAおよびUCPBのそれぞれの「コンテンツ

プロバイダのID」には、コンテンツプロバイダ2-1のIDが設定されている。「UCPのID」には、各UCPに割り当てられた所定のIDが設定され、UCPAの「UCPのID」には、UCPAのIDが、UCPBの「UCPのID」には、UCPBのIDが、それぞれ設定されている。「UCPの有効期限」には、UCPの有効期限を示す情報が設定され、UCPAの「UCPの有効期限」には、UCPAの有効期限が、UCPBの「UCPの有効期限」には、UCPBの有効期限が、それぞれ設定されている。

「利用条件」には、「ユーザ条件」および「機器条件」の各項目に対応する所定の情報が設定され、「ユーザ条件」には、このUCPを選択することができるユーザの条件が設定され、「機器条件」には、このUCPを選択することができる機器の条件が設定されている。

UCPAの場合、「利用条件10」が設定され、「利用条件10」の「ユーザ条件10」には、利用ポイントが200ポイント以上であることが条件であることを示す情報（”200ポイント以上”）が設定されている。また「利用条件10」の「機器条件10」には、条件がないことを示す情報（”条件なし”）が設定されている。すなわち、UCPAは、200ポイント以上のコンテンツプロバイダ2-1のコンテンツ利用ポイントを有するユーザのみが選択可能となる。

UCPBの場合、「利用条件20」が設定され、「利用条件20」の「ユーザ条件20」には、利用ポイントが200ポイントより少ないことが条件であることを示す情報（”200ポイントより少ない”）が設定されている。また「利用条件20」の「機器条件20」には、”条件なし”が設定されている。すなわち、UCPBは、200ポイントより少ないコンテンツプロバイダ2-1のコンテンツ利用ポイントを有するユーザのみが選択可能となる。

「利用内容」には、「ID」、「形式」、「パラメータ」、および「管理移動許可情報」の各項目に対応する所定の情報が含まれる。「ID」には、「利用内容」に設定される情報に割り当てられた所定のIDが設定される。「形式」には、再生や複製など、コンテンツの利用形式を示す情報が設定される。「パラメー

タ」には、「形式」に設定された利用形式に対応する所定の情報が設定される。

「管理移動許可情報」には、コンテンツの管理移動が可能か否か（許可されているか否か）を示す情報（”可”または”不可”）が設定される。コンテンツの管理移動が行われると、図 1 3 A に示すように、管理移動元の機器にコンテンツが保持されつつ、管理移動先の機器にそのコンテンツが移動される。すなわち、管理移動元の機器と管理移動先の機器の両方において、コンテンツが利用される。この点で、図 1 3 B に示すように、移動元の機器にコンテンツが保持されず、移動先の機器のみにコンテンツが保持され、移動先の機器においてのみコンテンツが利用される、通常の移動とは異なる。

また、コンテンツの管理移動が行われている間、管理移動元の機器は、図 1 3 A に示すように、他の機器にコンテンツを管理移動することができない（許可されていない）。すなわち、管理移動元の機器と管理移動先の機器の 2 機においてのみコンテンツが保持される。この点で、図 1 4 A に示すように、オリジナルのコンテンツから、複数の複製（第 1 世代）を作成することができる、第 1 世代の複製とも異なる。また、管理移動元の機器からコンテンツを戻すことより、他の機器にコンテンツを管理移動することができるので、この点で、図 1 4 B に示すように、1 回だけの複製とも異なる。

図 1 2 A に戻り、UCPA には、4 つの「利用内容 1 1」乃至「利用内容 1 4」が設けられており、「利用内容 1 1」において、その「ID 1 1」には、「利用内容 1 1」に割り当てられた所定の ID が設定されている。「形式 1 1」には、コンテンツを買い取って再生する利用形式を示す情報（”買い取り再生”）が設定され、「パラメータ 1 1」には、”買い取り再生”に対応する所定の情報が設定されている。「管理移動許可情報 1 1」には、コンテンツの管理移動が許可されていることを示す情報（”可”）が設定されている。

「利用内容 1 2」において、その「ID 1 2」には、「利用内容 1 2」に割り当てられた所定の ID が設定されている。「形式 1 2」には、第 1 世代の複製を行う利用形式を示す情報（”第 1 世代複製”）が設定されている。第 1 世代複製

は、図 1 4 A に示したように、オリジナルのコンテンツから、複数の第 1 世代の複製を作成することができる。ただし、第 1 世代の複製から第 2 世代の複製を作成することはできない（許可されていない）。「パラメータ 1 2」には、“第 1 世代複製”に対応する所定の情報が設定されている。「管理移動許可情報 1 2」には、コンテンツの管理移動が許可されていないことを示す情報（“不可”）が設定されている。

「利用内容 1 3」において、その「ID 1 3」には、「利用内容 1 3」に割り当てられた所定の ID が設定されている。「形式 1 3」には、所定の期間（時間）に限って再生する利用形式を示す情報（“期間制限再生”）が設定され、「パラメータ 1 3」には、“期間制限再生”に対応して、その期間の開始時期（時刻）と終了時期（時刻）が設定されている。「管理移動許可情報 1 3」には、“不可”が設定されている。

「利用内容 1 4」において、その「ID 1 4」には、「利用内容 1 4」に割り当てられた所定の ID が設定されている。「形式 1 4」には、5 回の複製を行う利用形式（いわゆる、5 回複製することができる回数券）を示す情報（“Pay Per Copy 5”）が設定されている。なお、この場合も、図 1 4 の B に示すように、複製からの複製を作成することはできない（許可されていない）。「パラメータ 1 4」には、複製が 5 回可能であることを示す情報（“複製 5 回”）が設定されている。「管理移動許可情報 1 4」には、“不可”が設定されている。

図 1 2 B の UCPB には、2 つの「利用内容 2 1」、および「利用内容 2 2」が設けられている。「利用内容 2 1」において、その「ID 2 1」には、「利用内容 2 1」に割り当てられた所定の ID が設定されている。「形式 2 1」には、4 回の再生を行う利用形式を示す情報（“Pay Per Play 4”）が設定され、「パラメータ 2 1」には、再生が 4 回可能であることを示す情報（“再生 4 回”）が設定されている。「管理移動許可情報 2 1」には、“不可”が設定されている。

「利用内容 2 2」において、その「ID 2 2」には、「利用内容 2 2」に割り

当てられた所定のIDが設定されている。「形式22」には、「Pay Per Copy 2」が設定され、「パラメータ22」には、「複製2回」が設定されている。「管理移動許可情報22」には、「不可」が設定されている。

ここで、UCPAおよびUCPBの内容を比較すると、200ポイント以上の利用ポイントを有するユーザは、4通りの利用内容11乃至利用内容14から利用内容を選択することができるのに対して、200ポイントより少ない利用ポイントを有するユーザは、2通りの利用内容21, 22からしか利用内容を選択することができないものとされている。

ところで、図12は、UCPAおよびUCPBを模擬的に表しているが、例えば、UCPAの「利用条件10」およびUCPBの「利用条件20」には、実際は、図15Aに示すサービスコード、および図15Bに示すコンディションコードの他、サービスコードに対応して数値や所定の種類を示すバリューコードがそれぞれ設定されている。

図16Aは、UCPA（図12A）の「利用条件10」の「ユーザ条件10」および「機器条件10」として設定されている各コードのコード値を表している。UCPAの「利用条件10」の「ユーザ条件10」は、「200ポイント以上」とされているので、「利用ポイントに関し条件有り」を意味する80xxhのサービスコード（図15A）が、このとき数値200を示す0000C8hのバリューコードが、そして「>=（以上）」を意味する06hのコンディションコード（図15B）が、ユーザ条件として設定されている。

UCPAの「機器条件10」は、「条件なし」とされているので、「条件なし」を意味する0000hのサービスコード（図15A）が、このとき何ら意味を持たないFFFFFFhのバリューコードが、そして「無条件」を意味する00hのコンディションコード（図15B）が、機器条件として設定されている。

図16Bは、UCPBの「利用条件20」の「ユーザ条件20」および「機器条件20」として設定されている各コードのコード値を表している。「ユーザ条件20」は、「200ポイントより少ない」とされているので、「利用ポイント

に関し条件有り”を意味する80 x x hのサービスコード（図15A）が、数値200を示す0000C8hのバリューコードが、そして”<（より小さい）”を意味する03hのコンディションコード（図15B）が、ユーザ条件として設定されている。

UCPBの「機器条件20」は、UCPAの「機器条件10」と同様に、”条件なし”とされ、同一のコード値が設定されているので、その説明は省略する。

図11に戻り、セキュアコンテナ作成部38は、例えば、図17に示すような、コンテンツA（コンテンツ鍵KcoAで暗号化されている）、コンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）、UCPA, B、および署名からなるコンテンツプロバイダセキュアコンテナを作成する。なお、署名は、送信したいデータ（この場合、コンテンツA（コンテンツ鍵KcoAで暗号化されている）、コンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）、およびUCPA, Bの全体）にハッシュ関数を適用して得られたハッシュ値が、コンテンツプロバイダの公開鍵暗号の秘密鍵（この場合、コンテンツプロバイダ2-1の秘密鍵Kscp）で暗号化されたものである。

セキュアコンテナ作成部38はまた、コンテンツプロバイダセキュアコンテナに、図18に示すコンテンツプロバイダ2-1の証明書を付してサービスプロバイダ3に送信する。この証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ2-1に対し割り付けた証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、およびコンテンツプロバイダ2-1の名前、コンテンツプロバイダ2-1の公開鍵Kpcp、並びにその署名（認証局の秘密鍵Kscaで暗号化されている）から構成されている。

署名は、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値とし

て出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4 (Message Digest), MD5, SHA (Secure Hash Algorithm) - 1などが用いられる。

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

公開鍵暗号の中で代表的なRSA (Rivest-Shamir-Adleman) 暗号を、簡単に説明する。まず、2つの十分に大きな素数である p および q を求め、さらに p と q の積である n を求める。 $(p-1)$ と $(q-1)$ の最小公倍数 L を算出し、更に、3以上 L 未満で、かつ、 L と互いに素な数 e を求める（すなわち、 e と L を共通に割り切れる数は、1のみである）。

次に、 L を法とする乗算に関する e の乗法逆元 d を求める。すなわち、 d 、 e 、および L の間には、 $ed = 1 \pmod{L}$ が成立し、 d はユークリッドの互除法で算出できる。このとき、 n と e が公開鍵とされ、 p 、 q 、および d が、秘密鍵とされる。

暗号文 C は、平文 M から、式(1)の処理で算出される。

$$C = M^e \bmod n \quad (1)$$

暗号文Cは、式(2)の処理で平文Mに、復号される。

$$M = C^d \bmod n \quad (2)$$

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式(3)が成立するからである。

$$M = C^d = (M^e)^d = M^{e \cdot d} = M \bmod n \quad (3)$$

秘密鍵pとqを知っているならば、公開鍵eから秘密鍵dは算出できるが、公開鍵nの素因数分解が計算量的に困難な程度に公開鍵nの桁数を大きくすれば、公開鍵nを知るだけでは、公開鍵eから秘密鍵dは計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

また、公開鍵暗号の他の例である楕円曲線暗号(Elliptic Curve Cryptography)についても、簡単に説明する。

楕円曲線 $y^2 = x^3 + ax + b$ 上の、ある点をBとする。楕円曲線上の点の加算を定義し、 nB は、Bをn回加算した結果を表す。同様に、減算も定義する。Bと nB からnを算出することは、困難であることが証明されている。Bと nB を公開鍵とし、nを秘密鍵とする。乱数rを用いて、暗号文C1およびC2は、平文Mから、公開鍵で式(4)および式(5)の処理で算出される。

$$C1 = M + r n B \quad (4)$$

$$C2 = r B \quad (5)$$

暗号文C 1およびC 2は、式(6)の処理で平文Mに、復号される。

$$M = C 1 - n C 2 \quad (6)$$

復号できるのは、秘密鍵nを有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

図11に、再び戻り、コンテンツプロバイダ2-1の相互認証部39は、EMDサービスセンタ1から配送用鍵Kdの供給を受けるのに先立ち、EMDサービスセンタ1と相互認証する。また相互認証部39は、サービスプロバイダ3へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ3と相互認証することも可能であるが、この例の場合、コンテンツプロバイダセキュアコンテナには、秘密しなければならない情報が含まれていないので、この相互認証は必ずしも必要とされるわけではない。

コンテンツプロバイダ2-2は、コンテンツプロバイダ2-1と基本的に同様の構成を有しているので、その図示および説明は省略する。

(4) サービスプロバイダ

次に、図19のブロック図を参照して、サービスプロバイダ3-1の機能的構成を説明する。コンテンツサーバ41は、コンテンツプロバイダ2から供給されたコンテンツプロバイダセキュアコンテナに含まれる、コンテンツ(コンテンツ鍵Kcoで暗号化されている)、コンテンツ鍵Kco(配送用鍵Kdで暗号化されている)、UCP、およびコンテンツプロバイダ2の署名を記憶し、セキュアコンテナ作成部44に供給する。

値付け部42は、コンテンツプロバイダ2から供給されたコンテンツプロバイダセキュアコンテナに含まれる署名に基づいて、コンテンツプロバイダセキュアコンテナの正当性を検証するが、この場合、コンテンツプロバイダ2の証明書が

検証され、正当であるとき、コンテンツプロバイダ 2 の公開鍵が取得される。そしてこの取得された公開鍵に基づいて、コンテンツプロバイダセキュアコンテナの正当性が検証される。

コンテンツプロバイダセキュアコンテナの正当性を確認すると、値付け部 4 2 は、コンテンツプロバイダセキュアコンテナに含まれる UCP に対応する、PT を作成し、セキュアコンテナ作成部 4 4 に供給する。図 20 は、図 12 (A) の UCPA に対応して作成された、2 つの PTA-1 (図 20 A) および PTA-2 (図 20 B) を表している。PT には、「コンテンツの ID」、「コンテンツプロバイダの ID」、「UCP の ID」、「サービスプロバイダの ID」、「PT の ID」、「PT の有効期限」、「価格条件」、および「価格内容」の各項目に対応する所定の情報が含まれる。

PT の、「コンテンツの ID」、「コンテンツプロバイダの ID」、および「UCP の ID」には、UCP に対応する項目の情報が、それぞれ設定される。すなわち、PTA-1 および PTA-2 のそれぞれの「コンテンツの ID」には、コンテンツ A の ID が、それぞれの「コンテンツプロバイダの ID」には、コンテンツプロバイダ 2-1 の ID が、そしてそれぞれの「UCP の ID」には、UCPA の ID が設定されている。

「サービスプロバイダの ID」には、PT の提供元のサービスプロバイダ 2 の ID が設定される。PTA-1 および PTA-2 のそれぞれの「サービスプロバイダの ID」には、サービスプロバイダ 3-1 の ID が設定されている。「PT の ID」には、各 PT に割り当てられた所定の ID が設定される。PTA-1 の「PT の ID」には、PTA-1 の ID が、PTA-2 の「PT の ID」には、PTA-2 の ID がそれぞれ設定されている。「PT の有効期限」には、PT の有効期限を示す情報が設定される。PTA-1 の「PT の有効期限」には、PTA-1 の有効期限が、PTA-2 の「PT の有効期限」には、PTA-2 の有効期限が設定されている。

「価格条件」には、UCP の「利用条件」と同様に、「ユーザ条件」および「機

器条件」の各項目に対応する所定の情報が設定されている。「価格条件」の「ユーザ条件」には、このPTを選択することができるユーザの条件を示す情報が設定され、その「機器条件」には、このPTを選択することができる機器の条件を示す情報が設定される。

PTA-1の場合、「価格条件10」が設定され、「価格条件10」の「ユーザ条件10」には、ユーザが男性であることを示す情報（”男性”）が設定され、その「機器条件10」には、”条件なし”が設定されている。すなわち、PTA-1は、男性のユーザのみが選択可能となる。

PTA-1の「価格条件10」の「ユーザ条件10」および「機器条件10」も、実際は、図21Aに示すように、各種コードのコード値が設定されている。「価格条件10」の「ユーザ条件10」には、”性別条件有り”を意味する01xxhのサービスコード（図15A）が、このとき男性を意味する000000hのバリューコードが、そして”=”を意味する01hのコンディションコード（図15B）が設定されている。「機器条件10」には、”条件なし”を意味する0000hのサービスコードが、この場合何ら意味を持たないFFFFFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコードが設定されている。

PTA-2の場合、「価格条件20」が設定され、「価格条件20」の「ユーザ条件20」には、ユーザが女性であることを示す情報（”女性”）が設定され、その「機器条件20」には、”条件なし”が設定されている。すなわち、PTA-2は、女性のユーザのみが選択可能となる。

PTA-2の「価格条件20」の「ユーザ条件20」および「機器条件20」も、実際は、図21Bに示すように、各コードのコード値が設定されている。「価格条件20」の「ユーザ条件20」には、”性別条件有り”を意味する01xxhのサービスコード（図15A）が、この場合女性を示す000001hのバリューコードが、そして”=”を意味する01hのコンディションコード（図15B）が設定されている。その「機器条件20」には、”条件なし”を意味する

0000hのサービスコードが、この場合何ら意味を持たないFFFFFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコードが設定されている。

図20に戻り、PTの「価格内容」には、コンテンツが、対応するUCPの「利用内容」の「形式」に設定されている利用形式で利用される場合の利用料金が示されている。すなわち、PTA-1の「価格内容11」に設定された”2000円”およびPTA-2の「価格内容21」に設定された”1000円”は、UCPA（図12A）の「利用内容11」の「形式11」が”買い取り再生”とされているので、コンテンツAの買い取り価格（料金）を示している。

PTA-1の「価格内容12」の”600円”およびPTA-2の「価格内容22」の”300円”は、UCPAの「利用内容12」の「形式12」より、第1世代複製の利用形式でコンテンツAを利用する場合の料金を示している。PTA-1の「価格内容13」の”100円”およびPTA-2の「価格内容23」の”50円”は、UCPAの「利用内容13」の「形式13」より、期間制限再生の利用形式でコンテンツAを利用する場合の料金を示している。PTA-1の「価格内容14」の”300円”およびPTA-2の「価格内容24」の”150円”は、UCPAの「利用内容14」の「形式14」より、5回の複製を行う利用形式でコンテンツAを利用する場合の料金を示している。

なお、この例の場合、PTA-1（男性ユーザに適用される）の価格内容と、PTA-2（女性ユーザに適用される）の価格内容を比較すると、PTA-1の価格内容に示される価格が、PTA-2の価格内容に示される価格の2倍に設定されている。例えば、UCPAの「利用内容11」に対応するPTA-1の「価格内容11」が”2000円”とされているのに対し、同様にUCPAの「利用内容11」に対応するPTA-2の「価格内容21」は”1000円”とされている。同様に、PTA-1の「価格内容12」乃至「価格内容14」に設定されている価格は、PTA-2の「価格内容22」乃至「価格内容24」に設定されている価格の2倍とされている。すなわち、コンテンツAは、女性のユーザがよ

り低価格で利用できるコンテンツとされている。

図 2 2 は、図 1 2 B の U C P B に対応して作成された、2 つの P T B - 1 および P T B - 2 を表している。図 2 2 A の P T B - 1 には、コンテンツ A の I D、コンテンツプロバイダ 2 - 1 の I D、U C P B の I D、サービスプロバイダ 3 - 1 の I D、P T B - 1 の I D、P T B - 1 の有効期限、価格条件 3 0、2 通りの価格内容 3 1、3 2 などが含まれている。

P T B - 1 の「価格条件 3 0」の「ユーザ条件 3 0」には”条件なし”が設定され、「機器条件 3 0」には、機器が従機器であることを条件とする情報（”従機器”）が設定されている。すなわち、P T B - 1 は、コンテンツ A が従機器において利用される場合にのみ選択可能となる。

P T B - 1 の「価格条件 3 0」の「ユーザ条件 3 0」および「機器条件 3 0」にも、実際は、図 2 3 A に示すように、各コードのコード値が設定されている。

「ユーザ条件 3 0」には、”条件なし”を意味する 0 0 0 0 h のサービスコード（図 1 5 A）が、この場合何ら意味を持たない F F F F F F h のバリューコードが、そして”無条件”を意味する 0 0 h のコンディションコード（図 1 5 B）が設定されている。「機器条件 3 0」は、”従機器”とされているので、”機器に関し条件有り”を意味する 0 0 x x h のサービスコードが、このとき”数値 1 0 0”を示す 0 0 0 0 6 4 h のバリューコードが、そして”<（小さい）”を意味する 0 3 h のコンディションコードが設定されている。この例の場合、従機器には、1 0 0 番より小さい機器番号が設定されているので、このようなコード値が設定される。

P T B - 1 の「価格内容 3 1」の”1 0 0 円”は、U C P B（図 1 2 B）の「利用内容 2 1」の「形式 2 1」が”Pay Per Play 4”とされているので、4 回の再生を行う場合の料金を示し、「価格内容 3 2」の”3 0 0 円”は、U C P B の「利用内容 2 2」の「形式 2 2」が”Pay Per Copy 2”とされているので、2 回の複製を行う場合の料金を示している。

U C P B に対応して作成された、もう一方の P T B - 2 には、図 2 2 B に示す

ように、コンテンツAのID、コンテンツプロバイダ2-1のID、UCPBのID、サービスプロバイダ3-1のID、PTB-2のID、PTB-2の有効期限、価格条件40、および2通りの価格内容41、42などが含まれている。

PTB-2の「価格条件40」の「ユーザ条件40」には”条件なし”が設定され、その「機器条件40」には、機器が主機器であることを条件とする情報（”主機器”）が設定されている。すなわち、PTB-2は、主機器においてコンテンツが利用される場合にのみ選択可能となる。

PTB-2の「価格条件40」の「ユーザ条件40」および「機器条件40」にも、実際は、図23Bに示すように、各コードのコード値が設定されている。

「価格条件40」の「ユーザ条件40」には、”条件なし”を意味する0000hのサービスコード（図15A）が、この場合何ら意味を持たないFFFFFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコード（15B）が設定されている。「機器条件40」には、”機器に関し条件有り”を意味する00xxhのサービスコードが、このとき”数値100”を示す000064hのバリューコードが、そして”=>（以上）”を意味する06hのコンディションコードが設定されている。この例の場合、主機器には、100番以上の機器番号が設定されているので、このようなコード値が設定される。

PTB-2の「価格内容41」および「価格内容42」のそれぞれに示される価格は、UCPBの「利用内容21」の「形式21」および「利用内容22」の「形式22」のそれぞれに示される利用形式でコンテンツAを利用する場合の料金を示している。

ここで、PTB-1（従機器に適用される）の価格内容とPTB-2（主機器に適用される）の価格内容を比較すると、PTB-1の価格内容は、PTB-2の価格内容の2倍に設定されている。例えば、PTB-1の「価格内容31」が”100円”とされているのに対し、PTB-2の「価格内容41」は50円とされており、「価格内容32」が”300円”とされているのに対して、「価格内容42」は”150円”とされている。

図 19 に戻り、ポリシー記憶部 43 は、コンテンツプロバイダ 2 から供給された、コンテンツの UCP を記憶し、セキュアコンテナ作成部 44 に供給する。

セキュアコンテナ作成部 44 は、例えば、図 24 に示すような、コンテンツ A（コンテンツ鍵 $K_{c \circ A}$ で暗号化されている）、コンテンツ鍵 $K_{c \circ A}$ （配送用鍵 K_d で暗号化されている）、UCPA、B、コンテンツプロバイダ 2 の署名、PTA-1、A-2、B-1、B-2、およびサービスプロバイダ 3 の署名からなるサービスプロバイダセキュアコンテナを作成する。

セキュアコンテナ作成部 44 はまた、作成したサービスプロバイダセキュアコンテナを、図 25 に示すような、証明書のバージョン番号、認証局がサービスプロバイダ 3-1 に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ 3-1 の名前、サービスプロバイダ 3-1 の公開鍵 K_{psp} 、並びに認証局の署名より構成されるサービスプロバイダの証明書を付して、ユーザホームネットワーク 5 に供給する。

図 19 に、再び戻り、相互認証部 45 は、コンテンツプロバイダ 2 からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ 2 と相互認証する。相互認証部 45 また、ユーザホームネットワーク 5 へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク 5 と相互認証するが、このサービスプロバイダ 3 とユーザホームネットワーク 5 との相互認証は、例えば、ネットワーク 4 が衛星通信である場合、実行されない。なお、この例の場合、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナには、特に、秘密情報が含まれていないので、サービスプロバイダ 3 は、コンテンツプロバイダ 2 およびユーザホームネットワーク 5 と相互認証を行わなくてもよい。

サービスプロバイダ 3-2 の構成は、サービスプロバイダ 3-1 の構成と基本的に同様であるので、その図示および説明は省略する。

(5) ユーザホームネットワーク

(5-1) レシーバ51

次に、図26のブロック図を参照して、ユーザホームネットワーク5を構成するレシーバ51の構成例を説明する。レシーバ51は、通信部61、SAM62、外部記憶部63、伸張部64、通信部65、インタフェース66、表示制御部67、および入力制御部68より構成されている。通信部61は、ネットワーク4を介してサービスプロバイダ3、またはEMDサービスセンタ1と通信し、所定の情報を受信し、または送信する。

SAM62は、相互認証モジュール71、課金処理モジュール72、記憶モジュール73、復号/暗号化モジュール74、およびデータ検査モジュール75からなるが、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有している。

SAM62の相互認証モジュール71は、記憶モジュール73に記憶されている、図27に示すSAM62の証明書を、相互認証相手に送信し、相互認証を実行し、これにより、認証相手と共有することとなった一時鍵 K_{temp} （セッション鍵）を復号/暗号化モジュール74に供給する。SAMの証明書には、コンテンツプロバイダ2-1の証明書およびサービスプロバイダ3-1の証明書に含まれている情報に対応する情報が含まれているので、その説明は省略する。

課金処理モジュール72は、選択されたUCPの利用内容に基づいて、使用許諾条件情報UCSおよびコンテンツが“買い取り再生”の利用形式で権利購入された場合のUCSの例であり、課金情報を作成する。図28は、図12Aに示したUCPAの利用内容11と、図20Aに示したPTA-1の価格内容11に基づいて作成されたUCSAを表している。UCSには、図28に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、

「利用内容」、および「利用履歴」の各項目に対応する所定の情報が設定される。

UCSの、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、および「PTの有効期限」の各項目には、PTの、それらに対応する項目の情報が設定される。すなわち、図28のUCSAの、「コンテンツのID」には、コンテンツAのIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ2-1のIDが、「UCPのID」には、UCPAのIDが、「UCPの有効期限」には、UCPAの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ3-1のIDが、「PTのID」には、PTA-1のIDが、そして「PTの有効期限」には、PTA-1の有効期限が、それぞれ設定されている。

「UCSのID」には、UCSに割り当てられた所定のIDが設定され、UCSAの「UCSのID」には、UCSAのIDが設定されている。「SAMのID」には、機器のSAMのIDが設定され、UCSAの「SAMのID」には、レシーバ51のSAM62のIDが設定されている。「ユーザのID」には、コンテンツを利用するユーザのIDが設定され、UCSAの「ユーザのID」には、ユーザFのIDが設定されている。

「利用内容」は、「ID」、「形式」、「パラメータ」、および「管理移動状態情報」の各項目からなり、そのうち「ID」、「形式」、および「パラメータ」の項目には、選択されたUCPの「利用内容」の、それらに対応する項目の情報が設定される。すなわち、UCSAの「ID」には、UCPAの「利用内容11」の「ID11」に設定されている情報（利用内容11のID）が、「形式」には、「利用内容11」の「形式11」に設定されている”買い取り再生”が、「パラメータ」には、「利用内容11」の「パラメータ11」に設定されている情報（”買い取り再生”に対応する情報）が設定されている。

「利用内容」の「管理移動状態情報」には、選択されたUCPの「管理移動許

可情報」に”可”が設定されている場合（管理移動が行える場合）、管理移動元の機器（コンテンツを購入した機器）と管理移動先の機器のそれぞれのIDが設定されるようになされている。なお、コンテンツの管理移動が行われていない状態においては、管理移動元の機器のIDが、管理移動先の機器のIDとしても設定される。一方、UCPの「管理移動許可情報」に、”不可”が設定されている場合、「管理移動状態情報」には”不可”が設定される。すなわち、この場合、コンテンツの管理移動は行われない（許可されない）。UCSAの「管理移動状態情報」には、UCPAの「利用内容11」の「管理移動許可情報11」に”可”が設定されており、また、このとき、コンテンツAは管理移動されていないので、SAM62のIDが、管理移動元の機器のIDおよび管理移動先の機器のIDとして設定されている。

「利用履歴」には、同一のコンテンツに対する利用形式の履歴が設定される。UCSAの「利用履歴」には、”買い取り再生”を示す情報のみが記憶されているが、例えば、レシーバ51において、コンテンツAが以前に利用されていた場合、そのときの利用形式も記憶される。

なお、上述したUCSにおいては、「UCPの有効期限」および「PTの有効期限」が設けられているがそれらをUCSに設定しないようにすることもできる。また、上述したUCSにおいて、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

作成されたUCSは、レシーバ51の復号／暗号化モジュール74の復号化ユニット91から供給されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）とともに、外部記憶部63に送信され、その利用情報記憶部63Aに記憶される。外部記憶部63の利用情報記憶部63Aは、図29に示すように、

M個のブロックBP-1乃至BP-Mに分割され（例えば、1メガバイト毎に分割され）、各ブロックBPが、N個の利用情報用メモリ領域RP-1乃至RP-Nに分割されている。SAM62から供給されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）およびUCSは、利用情報用記憶部63Aの所定のブロックBPの利用情報用メモリ領域RPに、対応して記憶される。

図29の例では、ブロックBP-1の利用情報用メモリ領域RP-3に、図28に示したUCSAと、コンテンツAを復号するためのコンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）が対応して記憶されている。ブロックBP-1の利用情報用メモリ領域RP-1、RP-2には、他のコンテンツ鍵Kco1、Kco2（それぞれ保存用鍵Ksaveで暗号化されている）およびUCS1、2がそれぞれ記憶されている。ブロックBP-1の利用情報用メモリ領域RP-4（図示せず）乃至RP-N、およびブロックBP-2（図示せず）乃至BP-Mには、この場合、コンテンツ鍵KcoおよびUCSは記憶されておらず、空いていることを示す所定の初期情報が記憶されている。なお、利用情報用メモリ領域RPに記憶されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）およびUCSを、個々に区別する必要がない場合、まとめて、利用情報と称する。

図30は、図28に示したUCSAと同時に作成された課金情報Aを表している。課金情報は、図30に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、「利用内容」、および「課金履歴」の各項目に対応する所定の情報が設定される。

課金情報の、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、および「利用内容」には、UCSの、それらに対応する項目の情報

が、それぞれ設定される。すなわち、図30の課金情報Aの、「コンテンツのID」には、コンテンツAのIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ2-1のIDが、「UCPのID」には、UCPAのIDが、「UCPの有効期限」には、UCPAの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ3-1のIDが、「PTのID」には、PTA-1のIDが、「PTの有効期限」には、PTA-1の有効期限が、「UCSのID」には、UCSAのIDが、「SAMのID」には、SAM62のIDが、「ユーザのID」には、ユーザFのIDが、そして「利用内容」には、UCSAの「利用内容11」の内容が、それぞれ設定されている。

課金情報の「課金履歴」には、機器において計上された課金の合計額を示す情報が設定される。課金情報Aの「課金履歴」には、レシーバ51において計上された課金の合計額が設定されている。

なお、上述した課金情報においては、「UCPの有効期限」および「PTの有効期限」が設けられているが、それらを課金情報に設定しないようにすることもできる。また、上述した課金情報においては、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

図26に戻り、記憶モジュール73には、図31に示すように、SAM62の公開鍵K_{pu}、SAM62の秘密鍵K_{su}、EMDサービスセンタ1の公開鍵K_{pesc}、認証局の公開鍵K_{pca}、保存用鍵K_{save}、3ヶ月分の配送用鍵K_dなどの各種鍵、SAM62の証明書(図27)、課金情報(例えば、図30の課金情報A)、基準情報51、およびM個の検査値HP-1乃至HP-Mなどが記憶されている。

図32は、記憶モジュール73に記憶されている基準情報51を表している。

基準情報には、「SAMのID」、「機器番号」、「決済ID」、「課金の上限額」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の各項目に設定される所定情報などが含まれている。

基準情報の、「SAMのID」、「機器番号」、「決済ID」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」には、EMDサービスセンタ1のユーザ管理部18により管理されるシステム登録情報（図9）の、それらに対応する項目の情報が、それぞれ設定される。すなわち、基準情報51には、SAM62のID、SAM62の機器番号（100番）、ユーザFの決済ID、ユーザFの決済ユーザ情報（ユーザFの一般情報（氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別）、ユーザFのID、およびユーザFのパスワード）、および図33に示す利用ポイント情報（図10に示したものと同様の情報）が設定されている。

「課金の上限額」には、機器がEMDシステムに正式登録されている状態と仮登録されている状態で、それぞれ異なる課金の上限額が設定される。基準情報51の「課金の上限額」には、レシーバ51が正式登録されているので、正式登録されている状態における課金の上限額を示す情報（“正式登録時の上限額”）が設定されている。なお、正式登録されている状態における課金の上限額は、仮登録されている状態における課金の上限額よりも、大きな額である。

次に、記憶モジュール73に記憶される、図31に示したM個の検査値HP-1乃至HP-Mについて説明する。検査値HP-1は、外部記憶部63の利用情報記憶部63AのブロックBP-1に記憶されているデータの全体にハッシュ関数が適用されて算出されたハッシュ値である。検査値HP-2乃至HP-Mも、検査値HP-1と同様に、外部記憶部63の、対応するブロックBP-2乃至BP-Mのそれぞれに記憶されているデータのハッシュ値である。

図26に戻り、SAM62の復号/暗号化モジュール74は、復号ユニット91、乱数発生ユニット92、および暗号化ユニット93から構成される。復号ユニット91は、暗号化されたコンテンツ鍵Kcoを配送用鍵Kdで復号し、暗号

化ユニット 9 3 に出力する。乱数発生ユニット 9 2 は、必要に応じ（例えば、相互認証時に）、所定の桁数の乱数を発生し、一時鍵 K_{temp} を生成し、暗号化ユニット 9 3 に出力する。

暗号化ユニット 9 3 は、復号されたコンテンツ鍵 $K_c o$ を、再度、記憶モジュール 7 3 に保持されている保存用鍵 K_{save} で暗号化する。暗号化されたコンテンツ鍵 $K_c o$ は、外部記憶部 6 3 に供給される。暗号化ユニット 9 3 は、コンテンツ鍵 $K_c o$ を伸張部 6 4 に送信するとき、コンテンツ鍵 $K_c o$ を乱数発生ユニット 9 2 で生成した一時鍵 K_{temp} で暗号化する。

データ検査モジュール 7 5 は、記憶モジュール 7 3 に記憶されている検査値 H_P と、外部記憶部 6 3 の利用情報記憶部 6 3 A の、対応するブロック B_P のデータのハッシュ値を比較し、ブロック B_P のデータが改竄されていないか否かを検査する。データ検査モジュール 7 5 はまた、コンテンツの購入、利用、および管理移動等が行われる際に、検査値 H_P を算出し、記憶モジュール 7 3 に記憶（更新）させる。

伸張部 6 4 は、相互認証モジュール 1 0 1、復号モジュール 1 0 2、復号モジュール 1 0 3、伸張モジュール 1 0 4、およびウォーターマーク付加モジュール 1 0 5 から構成される。相互認証モジュール 1 0 1 は、 $SAM62$ と相互認証し、一時鍵 K_{temp} を復号モジュール 1 0 2 に出力する。復号モジュール 1 0 2 は、一時鍵 K_{temp} で暗号化されたコンテンツ鍵 $K_c o$ を一時鍵 K_{temp} で復号し、復号モジュール 1 0 3 に出力する。復号モジュール 1 0 3 は、 $HDD52$ に記録されたコンテンツをコンテンツ鍵 $K_c o$ で復号し、伸張モジュール 1 0 4 に出力する。伸張モジュール 1 0 4 は、復号されたコンテンツを、更に $ATRA C2$ 等の方式で伸張し、ウォーターマーク付加モジュール 1 0 5 に出力する。ウォーターマーク付加モジュール 1 0 5 は、コンテンツにレシーバ 5 1 を特定するための情報（例えば、 $SAM62$ の ID ）のウォーターマーク（電子透かし）を挿入し、図示せぬスピーカに出力し、音楽を再生する。

通信部 6 5 は、ユーザホームネットワーク 5 のレシーバ 2 0 1 との通信処理を

行う。インターフェース 6 6 は、S A M 6 2 および伸張部 6 4 からの信号を所定の形式に変更し、H D D 5 2 に出力し、また、H D D 5 2 からの信号を所定の形式に変更し、S A M 6 2 および伸張部 6 4 に出力する。

表示制御部 6 7 は、表示部（図示せず）への出力を制御する。入力制御部 6 8 は、各種ボタンなどから構成される操作部（図示せず）からの入力を制御する。

H D D 5 2 は、サービスプロバイダ 3 から供給されたコンテンツの他、図 3 4 に示すような登録リストを記憶している。この登録リストは、表形式に情報が記憶されているリスト部、および登録リストを保持する機器についての所定の情報が記憶されている対象 S A M 情報部より構成されている。

対象 S A M 情報部には、この登録リストを保有する機器の S A M I D、この例の場合、レシーバ 5 1 の S A M 6 2 の I D が（「対象 S A M I D」の欄に）記憶されている。対象 S A M 情報部にはまた、この登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ 5 1 は、レシーバ 2 0 1 に接続されているので、自分自身を含む値 2 が（「接続されている機器数」の欄に）記憶されている。

リスト部は、「S A M I D」、「ユーザ I D」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、「状態フラグ」、「登録条件署名」、および「登録リスト署名」の 9 個の項目から構成され、この例の場合、レシーバ 5 1 の登録条件として、それぞれの項目に所定の情報が記憶されている。

「S A M I D」には、機器の S A M の I D が記憶される。この例の場合、レシーバ 5 1 の S A M 6 2 の I D およびレシーバ 2 0 1 の S A M 2 1 2 の I D が記憶されている。「ユーザ I D」には、対応する機器のユーザの I D が記憶される。この例の場合、ユーザ F の I D およびユーザ A の I D が記憶されている。

「購入処理」には、対応する機器が、コンテンツを購入（正確には、コンテンツを利用する権利を購入）するための処理を行うことができるか否かを示す情報（“可”または“不可”）が記憶される。この例の場合、レシーバ 5 1 およびレ

シーバ 201 は、コンテンツを購入するための処理を行うことができるので、“可” が記憶されている。

「課金処理」には、対応する機器が、EMD サービスセンタ 1 との間で、課金を決済する処理を行うことができるか否かを示す情報（“可” または“不可”）が記憶される。この例の場合、レシーバ 51 は、ユーザ F が決済ユーザとして登録されており、レシーバ 201 は、ユーザ A が決済ユーザとして登録されているので、課金を決済する処理を行うことができる。そのため、「課金処理」には、“可” が記憶されている。

「課金機器」には、対応する機器において計上された課金に対する課金を決済する処理を行う機器の SAM の ID が記憶される。この例の場合、レシーバ 51（SAM 62）およびレシーバ 201（SAM 212）は、自分自身の課金に対する決済を行うことができるので、SAM 62 の ID および SAM 212 の ID が記憶されている。

「コンテンツ供給機器」には、対応する機器が、コンテンツの供給をサービスプロバイダ 3 からではなく、接続される他の機器から受ける場合、コンテンツを供給することができる機器の SAM の ID が記憶される。この例の場合、レシーバ 51 およびレシーバ 201 は、コンテンツの供給をサービスプロバイダ 3 から受けるので、コンテンツを供給する機器が存在しない旨を示す情報（“なし”）が記憶されている。なお、ここで意味するコンテンツの供給は、管理移動によるものは含まれない。

「状態フラグ」には、対応する機器の動作制限条件が記憶される。何ら制限されていない場合は、その旨を示す情報（“制限なし”）、一定の制限が課せられている場合は、その旨を示す情報（“制限あり”）、また動作が停止させられている場合には、その旨を示す情報（“停止”）が記憶される。例えば、決済が成功しなかった場合、その機器に対応する「状態フラグ」には、“制限あり”が設定される。この例の場合、「状態フラグ」に“制限あり”が設定された機器においては、すでに購入されたコンテンツを利用する処理は実行されるが、新たなコ

ンテンツを購入するための処理は実行されなくなる。すなわち、一定の制限が機器に課せられる。また、コンテンツの不正複製などの違反行為が発覚した場合、「状態フラグ」には、「停止」が設定され、機器の動作が停止される。これにより、その機器はEMDシステムからのサービスを、一切受けることができなくなる。

この例の場合、レシーバ51およびレシーバ201に対しては、何ら制限が課せられていないものとし、「状態フラグ」には「なし」が設定されている。

「登録条件署名」には、登録条件として、それぞれ、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、および「状態フラグ」に記憶されている情報に対するEMDサービスセンタ1による署名が記憶されている。この例の場合、レシーバ51およびレシーバ201の登録条件に対する署名が記憶されている。

「登録リスト署名」には、登録リストに設定されているデータの全体に対する署名が設定されている。

(5-2) レシーバ201

図35は、レシーバ201の構成例を表している。レシーバ201の通信部211乃至入力制御部218は、レシーバ51の通信部61乃至入力制御部68と同様の機能を有しているので、その詳細な説明は適宜省略する。

外部記憶部213は、図36に示すように、P個のブロックBM-1乃至BM-Pに分割され（例えば、1メガバイト毎に分割され）、各ブロックBMが、Q個の移動情報用メモリ領域RM-1乃至RM-Qに分割されている移動情報記憶部213Aを有しており、例えば、コンテンツが管理移動されたとき、SAM212から送信される、そのコンテンツに対応したコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）、コンテンツのID、および管理移動元の機器のSAMのID（以下、個々に区別する必要がない場合、これらをまとめて、移動情報と称する）を記憶する。

図36の移動情報記憶部213AのブロックBM-1の移動情報用メモリ領域

RM-2には、コンテンツA（コンテンツ鍵K_{co}で暗号化されている）に対応するコンテンツ鍵K_{coA}（保存用鍵K_{save}で暗号化されている）、コンテンツAのID、およびSAM62のIDが記憶されている。すなわち、レシーバ51から、コンテンツAが管理移動されている状態の移動情報記憶部213Aを表している。

なお、ブロックBM-1の移動情報用メモリ領域RM-2（図示せず）乃至RM-Q、およびブロックBM-2（図示せず）乃至BM-Pには、移動情報が記憶されておらず、空いている（移動情報を記憶することができる）ことを示す初期情報が記憶されている。

SAM212の記憶モジュール223には、図37に示すように、SAM212の公開鍵K_{pu}、SAM212の秘密鍵K_{su}、EMDサービスセンタ1の公開鍵K_{pesc}、認証局の公開鍵K_{pca}、保存用鍵K_{save}、3ヶ月分の配送用鍵K_d、予め認証局から配布されているSAM212の証明書、基準情報201、およびQ個の検査値HM-1乃至HM-Qが記憶されている。

P個の検索値HM-1乃至HM-Qは、外部記憶部213の移動情報記憶部213Aの、各ブロックBM-1乃至BM-Qの記憶されているデータにハッシュ関数が適用されて算出されたハッシュ値である。

HDD202は、HDD52と同様の機能を有するので、その説明は省略するが、HDD202には、図34のレシーバ51の登録リストのリスト部に示された、レシーバ51の登録条件およびレシーバ201の登録条件が設定されたリスト部を有するレシーバ201の登録リスト（図示せず）が記憶されている。

なお、この例の場合、簡単のために、レシーバ51の外部記憶部63には、利用情報記憶部63Aのみが設けられ、またレシーバ201の外部記憶部213には、移動情報記憶部213Aのみが設けられているようにしたが、実際は、レシーバ51の外部記憶部63には、利用情報記憶部63Aの他、移動情報記憶部（図示せず）も設けられている。同様に、レシーバ201の外部記憶部213にも、移動情報記憶部213Aの他、利用情報記憶部（図示せず）が設けられている。

。

(6) コンテンツの購入及び利用

次に、EMDシステムの処理について、図38のフローチャートを参照して説明するが、ここでは、コンテンツプロバイダ2-1に保持されているコンテンツAが、サービスプロバイダ3-1を介して、ユーザホームネットワーク5のレシーバ51に供給され、利用される場合を例として説明する。

(6-1) EMDサービスセンタからコンテンツプロバイダへの配送用鍵の伝送

ステップS11において、配送用鍵Kdが、EMDサービスセンタ1からコンテンツプロバイダ2-1に供給される処理が行われる。この処理の詳細は、図39のフローチャートに示されている。すなわち、ステップS31において、EMDサービスセンタ1の相互認証部17(図3)は、コンテンツプロバイダ2-1の相互認証部39(図11)と相互認証し、コンテンツプロバイダ2-1が、正当なプロバイダであることが確認した後、EMDサービスセンタ1のコンテンツプロバイダ管理部12は、鍵サーバ14から供給された配送用鍵Kdをコンテンツプロバイダ2-1に送信する。なお、相互認証処理の詳細は、図40乃至図42を参照して後述する。

次に、ステップS32において、コンテンツプロバイダ2-1の暗号化部36は、EMDサービスセンタ1から送信された配送用鍵Kdを受信し、ステップS33において、配送用鍵Kdを記憶する。

このように、コンテンツプロバイダ2-1の暗号化部36が、配送用鍵Kdを記憶したとき、処理は終了し、図38のステップS12に進む。ここで、ステップS12以降の処理の説明の前に、図39のステップS31における相互認証処理(なりすましがいないことを確認する処理)について、1つの共通鍵を用いる場合(図40)、2つの共通鍵を用いる場合(図41)、および公開鍵暗号を用いる場合(図42)を例として説明する。

図40は、1つの共通鍵で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相

互認証の動作を説明するフローチャートである。ステップS 4 1において、コンテンツプロバイダ2の相互認証部3 9は、6 4ビットの乱数R 1を生成する（乱数生成部3 5が生成するようにしてもよい）。ステップS 4 2において、コンテンツプロバイダ2の相互認証部3 9は、DESを用いて乱数R 1を、予め記憶している共通鍵K cで暗号化する（暗号化部3 6で暗号化するようにしてもよい）。ステップS 4 3において、コンテンツプロバイダ2の相互認証部3 9は、暗号化された乱数R 1をEMDサービスセンタ1の相互認証部1 7に送信する。

ステップS 4 4において、EMDサービスセンタ1の相互認証部1 7は、受信した乱数R 1を予め記憶している共通鍵K cで復号する。ステップS 4 5において、EMDサービスセンタ1の相互認証部1 7は、3 2ビットの乱数R 2を生成する。ステップS 4 6において、EMDサービスセンタ1の相互認証部1 7は、復号した6 4ビットの乱数R 1の下位3 2ビットを乱数R 2で入れ替え、接続 $R_{1_H} \parallel R_2$ を生成する。なお、ここで R_{i_H} は、 R_i の上位nビットを表し、 $A \parallel B$ は、AとBの接続（nビットのAの下位に、mビットのBを結合して、 $(n + m)$ ビットとしたもの）を表す。ステップS 4 7において、EMDサービスセンタ1の相互認証部1 7は、DESを用いて $R_{1_H} \parallel R_2$ を共通鍵K cで暗号化する。ステップS 4 8において、EMDサービスセンタ1の相互認証部1 7は、暗号化した $R_{1_H} \parallel R_2$ をコンテンツプロバイダ2に送信する。

ステップS 4 9において、コンテンツプロバイダ2の相互認証部3 9は、受信した $R_{1_H} \parallel R_2$ を共通鍵K cで復号する。ステップS 5 0において、コンテンツプロバイダ2の相互認証部3 9は、復号した $R_{1_H} \parallel R_2$ の上位3 2ビット R_{1_H} を調べ、ステップS 4 1で生成した、乱数R 1の上位3 2ビット R_{1_H} と一致すれば、EMDサービスセンタ1が正当なセンタであることを認証する。生成した乱数 R_{1_H} と、受信した R_{1_H} が一致しないとき、処理は終了される。両者が一致するとき、ステップS 5 1において、コンテンツプロバイダ2の相互認証部3 9は、3 2ビットの乱数R 3を生成する。ステップS 5 2において、コンテンツプロバイダ2の相互認証部3 9は、受信し復号した $R_{1_H} \parallel R_2$ から下位3 2ビ

ットを取り出した乱数R2を上位に設定し、生成した乱数R3をその下位に設定し、接続R2 || R3とする。ステップS53において、コンテンツプロバイダ2の相互認証部39は、DESを用いて接続R2 || R3を共通鍵Kcで暗号化する。ステップS54において、コンテンツプロバイダ2の相互認証部39は、暗号化された接続R2 || R3をEMDサービスセンタ1の相互認証部17に送信する。

ステップS55において、EMDサービスセンタ1の相互認証部17は、受信した接続R2 || R3を共通鍵Kcで復号する。ステップS56において、EMDサービスセンタ1の相互認証部17は、復号した接続R2 || R3の上位32ビットを調べ、乱数R2と一致すれば、コンテンツプロバイダ2を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

図41は、2つの共通鍵Kc1, Kc2で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS61において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数R1を生成する。ステップS62において、コンテンツプロバイダ2の相互認証部39は、DESを用いて乱数R1を予め記憶している共通鍵Kc1で暗号化する。ステップS63において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数R1をEMDサービスセンタ1に送信する。

ステップS64において、EMDサービスセンタ1の相互認証部17は、受信した乱数R1を予め記憶している共通鍵Kc1で復号する。ステップS65において、EMDサービスセンタ1の相互認証部17は、乱数R1を予め記憶している共通鍵Kc2で暗号化する。ステップS66において、EMDサービスセンタ1の相互認証部17は、64ビットの乱数R2を生成する。ステップS67において、EMDサービスセンタ1の相互認証部17は、乱数R2を共通鍵Kc2で暗号化する。ステップS68において、EMDサービスセンタ1の相互認証部17は、暗号化された乱数R1および乱数R2をコンテンツプロバイダ2の相互認

証部 3 9 に送信する。

ステップ S 6 9 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、受信した乱数 R 1 および乱数 R 2 を予め記憶している共通鍵 K c 2 で復号する。ステップ S 7 0 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、復号した乱数 R 1 を調べ、ステップ S 6 1 で生成した乱数 R 1 (暗号化する前の乱数 R 1) と一致すれば、EMD サービスセンタ 1 を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップ S 7 1 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、復号して得た乱数 R 2 を共通鍵 K c 1 で暗号化する。ステップ S 7 2 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、暗号化された乱数 R 2 を EMD サービスセンタ 1 に送信する。

ステップ S 7 3 において、EMD サービスセンタ 1 の相互認証部 1 7 は、受信した乱数 R 2 を共通鍵 K c 1 で復号する。ステップ S 7 4 において、EMD サービスセンタ 1 の相互認証部 1 7 は、復号した乱数 R 2 が、ステップ S 6 6 で生成した乱数 R 2 (暗号化する前の乱数 R 2) と一致すれば、コンテンツプロバイダ 2 を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

図 4 2 は、公開鍵暗号である、1 6 0 ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ 2 の相互認証部 3 9 と EMD サービスセンタ 1 の相互認証部 1 7 との相互認証の動作を説明するフローチャートである。ステップ S 8 1 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、6 4 ビットの乱数 R 1 を生成する。ステップ S 8 2 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、自分自身の公開鍵 K p c p を含む証明書 (認証局から予め取得しておいたもの) と、乱数 R 1 を EMD サービスセンタ 1 の相互認証部 1 7 に送信する。

ステップ S 8 3 において、EMD サービスセンタ 1 の相互認証部 1 7 は、受信した証明書の署名 (認証局の秘密鍵 K s c a で暗号化されている) を、予め取得しておいた認証局の公開鍵 K p c a で復号し、コンテンツプロバイダ 2 の公開鍵 K p c p とコンテンツプロバイダ 2 の名前のハッシュ値を取り出すとともに、証

明書に平文のまま格納されているコンテンツプロバイダ 2 の公開鍵 $K_{p c p}$ およびコンテンツプロバイダ 2 の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵 $K_{p c p}$ およびコンテンツプロバイダ 2 の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ 2 の公開鍵 $K_{p c p}$ およびコンテンツプロバイダ 2 の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵 $K_{p c p}$ が改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

適正な認証結果が得られたとき、ステップ S 8 4 において、EMD サービスセンタ 1 の相互認証部 1 7 は、64 ビットの乱数 R_2 を生成する。ステップ S 8 5 において、EMD サービスセンタ 1 の相互認証部 1 7 は、乱数 R_1 および乱数 R_2 の接続 $R_1 \parallel R_2$ を生成する。ステップ S 8 6 において、EMD サービスセンタ 1 の相互認証部 1 7 は、接続 $R_1 \parallel R_2$ を自分自身の秘密鍵 $K_{s e s c}$ で暗号化する。ステップ S 8 7 において、EMD サービスセンタ 1 の相互認証部 1 7 は、接続 $R_1 \parallel R_2$ を、ステップ S 8 3 で取得したコンテンツプロバイダ 2 の公開鍵 $K_{p c p}$ で暗号化する。ステップ S 8 8 において、EMD サービスセンタ 1 の相互認証部 1 7 は、秘密鍵 $K_{s e s c}$ で暗号化された接続 $R_1 \parallel R_2$ 、公開鍵 $K_{p c p}$ で暗号化された接続 $R_1 \parallel R_2$ 、および自分自身の公開鍵 $K_{p e s c}$ を含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ 2 の相互認証部 3 9 に送信する。

ステップ S 8 9 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、受信した証明書の署名を予め取得しておいた認証局の公開鍵 $K_{p c a}$ で復号し、正しければ証明書から公開鍵 $K_{p e s c}$ を取り出す。この場合の処理は、ステップ S 8 3 における場合と同様であるので、その説明は省略する。ステップ S 9 0 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、EMD サービスセンタ 1 の

秘密鍵 $K_{se\ sc}$ で暗号化されている接続 $R_1 \parallel R_2$ を、ステップS 8 9で取得した公開鍵 $K_{pe\ sc}$ で復号する。ステップS 9 1において、コンテンツプロバイダ2の相互認証部3 9は、自分自身の公開鍵 $K_{pc\ p}$ で暗号化されている接続 $R_1 \parallel R_2$ を、自分自身の秘密鍵 $K_{sc\ p}$ で復号する。ステップS 9 2において、コンテンツプロバイダ2の相互認証部3 9は、ステップS 9 0で復号された接続 $R_1 \parallel R_2$ と、ステップS 9 1で復号された接続 $R_1 \parallel R_2$ を比較し、一致すればEMDサービスセンタ1を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

適正な認証結果が得られたとき、ステップS 9 3において、コンテンツプロバイダ2の相互認証部3 9は、64ビットの乱数 R_3 を生成する。ステップS 9 4において、コンテンツプロバイダ2の相互認証部3 9は、ステップS 9 0で取得した乱数 R_2 および生成した乱数 R_3 の接続 $R_2 \parallel R_3$ を生成する。ステップS 9 5において、コンテンツプロバイダ2の相互認証部3 9は、接続 $R_2 \parallel R_3$ を、ステップS 8 9で取得した公開鍵 $K_{pe\ sc}$ で暗号化する。ステップS 9 6において、コンテンツプロバイダ2の相互認証部3 9は、暗号化した接続 $R_2 \parallel R_3$ をEMDサービスセンタ1の相互認証部1 7に送信する。

ステップS 9 7において、EMDサービスセンタ1の相互認証部1 7は、暗号化された接続 $R_2 \parallel R_3$ を自分自身の秘密鍵 $K_{se\ sc}$ で復号する。ステップS 9 8において、EMDサービスセンタ1の相互認証部1 7は、復号した乱数 R_2 が、ステップS 8 4で生成した乱数 R_2 （暗号化する前の乱数 R_2 ）と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不適正なプロバイダとして、処理を終了する。

以上のように、EMDサービスセンタ1の相互認証部1 7とコンテンツプロバイダ2の相互認証部3 9は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵 K_{temp} として利用される。

(6-2) コンテンツプロバイダからサービスプロバイダへのコンテンツの伝送
次に、図3 8のステップS 1 2の処理について説明する。ステップS 1 2にお

いては、コンテンツプロバイダセキュアコンテナが、コンテンツプロバイダ2-1からサービスプロバイダ3-1に供給される処理が行われる。その処理の詳細は、図43のフローチャートに示されている。すなわち、ステップS201において、コンテンツプロバイダ2-1のウォーターマーク付加部32（図11）は、コンテンツサーバ31からコンテンツAを読み出し、コンテンツプロバイダ2-1を示す所定のウォーターマーク（電子透かし）を挿入し、圧縮部33に供給する。

ステップS202において、コンテンツプロバイダ2-1の圧縮部33は、ウォーターマークが挿入されたコンテンツAをATrac2等の所定の方式で圧縮し、暗号化部34に供給する。ステップS203において、乱数発生部35は、コンテンツ鍵KcoAとなる乱数を発生させ、暗号化部34に供給する。

ステップS204において、コンテンツプロバイダ2-1の暗号化部34は、DESなどの所定の方式で、乱数発生部35で発生された乱数（コンテンツ鍵KcoA）を使用して、ウォーターマークが挿入されて圧縮されたコンテンツAを暗号化する。次に、ステップS205において、暗号化部36は、DESなどの所定の方式で、EMDサービスセンタ1から供給された配送用鍵Kdでコンテンツ鍵KcoAを暗号化する。

ステップS206において、コンテンツプロバイダ2-1のセキュアコンテナ作成部38は、コンテンツA（コンテンツ鍵KcoAで暗号化されている）、コンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）、およびポリシー記憶部37に記憶されている、コンテンツAに対応するUCPA, B（図12）の全体にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵Kscpで暗号化する。これにより、図17に示した署名が作成される。

ステップS207において、コンテンツプロバイダ2-1のセキュアコンテナ作成部38は、コンテンツA（コンテンツ鍵KcoAで暗号化されている）、コンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）、UCPA, B（図12）、およびステップS206で生成した署名を含んだ、図17に示したコンテ

ンツプロバイダセキュアコンテナを作成する。

ステップS 2 0 8において、コンテンツプロバイダ2-1の相互認証部3 9は、サービスプロバイダ3-1の相互認証部4 5（図1 9）と相互認証する。この認証処理は、図4 0乃至図4 2を参照して説明した場合と同様であるので、その説明は省略する。ステップS 2 0 9において、コンテンツプロバイダ2-1のセキュアコンテナ作成部3 8は、認証局から予め発行された証明書（図1 8）を、ステップS 2 0 7で作成したコンテンツプロバイダセキュアコンテナに付して、サービスプロバイダ3-1に送信する。

このようにして、コンテンツプロバイダセキュアコンテナが、サービスプロバイダ3-1に供給されたとき、処理は終了し、図3 8のステップS 1 3に進む。

（6-3）サービスプロバイダからレシーバへのコンテンツの伝送

ステップS 1 3において、サービスプロバイダセキュアコンテナが、サービスプロバイダ3-1からユーザホームネットワーク5（レシーバ5 1）に供給される。この処理の詳細は、図4 4のフローチャートに示されている。すなわち、ステップS 2 2 1において、サービスプロバイダ3-1の値付け部4 2（図1 9）は、コンテンツプロバイダ2-1から送信されたコンテンツプロバイダセキュアコンテナに付された証明書（図1 8）に含まれる署名を確認し、証明書の改竄がなければ、それから、コンテンツプロバイダ2-1の公開鍵 $K_{p\ c\ p}$ を取り出す。証明書の署名の確認は、図4 2のステップS 8 3における処理と同様であるので、その説明は省略する。

ステップS 2 2 2において、サービスプロバイダ3-1の値付け部4 2は、コンテンツプロバイダ2-1から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ2-1の公開鍵 $K_{p\ c\ p}$ で復号し、得られたハッシュ値が、コンテンツA（コンテンツ鍵 $K_{c\ o\ A}$ で暗号化されている）、コンテンツ鍵 $K_{c\ o\ A}$ （配送用鍵 K_d で暗号化されている）、およびUCPA、Bの全体にハッシュ関数を適用して得られたハッシュ値と一致するか否かを判定し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。両者の値

が一致しない場合（改竄が発見された場合）は、処理は終了されるが、この例の場合、コンテンツプロバイダセキュアコンテナの改竄はなかったものとし、ステップS 2 2 3に進む。

ステップS 2 2 3において、サービスプロバイダ3-1の値付け部4 2は、コンテンツプロバイダセキュアコンテナから、コンテンツA（コンテンツ鍵K c o Aで暗号化されている）、コンテンツ鍵K c o A（配送用鍵K dで暗号化されている）、および署名を取り出し、コンテンツサーバ4 1に供給する。コンテンツサーバ4 1は、それらを記憶する。値付け部4 2はまたUCPA, Bも、コンテンツプロバイダセキュアコンテナから取り出し、セキュアコンテナ作成部4 4に供給する。

ステップS 2 2 4において、サービスプロバイダ3-1の値付け部4 2は、取り出したUCPA, Bに基づいて、PTA-1, A-2（図2 0）、およびPTB-1, B-2（図2 2）を作成し、セキュアコンテナ作成部4 4に供給する。

ステップS 2 2 5において、サービスプロバイダ3-1のセキュアコンテナ作成部4 4は、コンテンツサーバ4 1から読み出したコンテンツA（コンテンツ鍵K c o Aで暗号化されている）およびコンテンツ鍵K c o A（配送用鍵K dで暗号化されている）と、値付け部4 2から供給された、UCPA, B、およびPTA-1, A-2, B-1, B-2、並びにその署名から、図2 4に示したサービスプロバイダセキュアコンテナを作成する。

ステップS 2 2 6において、サービスプロバイダ3-1の相互認証部4 5は、レシーバ5 1の相互認証モジュール7 1（図2 6）と相互認証する。この認証処理は、図4 0乃至図4 2を参照して説明した場合と同様であるので、その説明を省略する。

ステップS 2 2 7において、サービスプロバイダ3-1のセキュアコンテナ作成部4 4は、ステップS 2 2 5で作成したサービスプロバイダセキュアコンテナに、サービスプロバイダ3-1の証明書（図2 5）を付して、ユーザホームネットワーク5のレシーバ5 1に送信する。

このようにして、サービスプロバイダセキュアコンテナが、サービスプロバイダ 3-1 からレシーバ 5 1 に送信されたとき、処理は終了し、図 3 8 のステップ S 1 4 に進む。

(6-4) レシーバによるコンテンツの記録処理

ステップ S 1 4 において、サービスプロバイダ 3-1 から送信されたサービスプロバイダセキュアコンテナが、ユーザホームネットワーク 5 のレシーバ 5 1 により受信される。この処理の詳細は、図 4 5 のフローチャートに示されている。すなわち、ステップ S 2 4 1 において、レシーバ 5 1 の相互認証モジュール 7 1

(図 2 6) は、通信部 6 1 を介して、サービスプロバイダ 3-1 の相互認証部 4 5 (図 1 9) と相互認証し、相互認証できたとき、通信部 6 1 は、相互認証したサービスプロバイダ 3-1 から、サービスプロバイダセキュアコンテナ (図 2 4) を受信する。相互認証できなかった場合、処理は終了されるが、この例の場合、相互認証されたものとし、ステップ S 2 4 2 に進む。

ステップ S 2 4 2 において、レシーバ 5 1 の通信部 6 1 は、ステップ S 2 4 1 で相互認証したサービスプロバイダ 3-1 から、公開鍵証明書を受信する。

ステップ S 2 4 3 において、レシーバ 5 1 の復号/暗号化モジュール 7 4 は、ステップ S 2 4 1 で受信したサービスプロバイダセキュアコンテナに含まれる署名を検証し、改竄がなかったか否かを検証する。ここで、改竄が発見された場合、処理は終了するが、この例の場合、改竄が発見されなかったものとし、ステップ S 2 4 4 に進む。

ステップ S 2 4 4 において、レシーバ 5 1 の記憶モジュール 7 3 に記憶されている基準情報 5 1 (図 3 2) に基づいて、利用条件を満たす U C P と価格条件を満たす P T が選択され、表示制御部 6 7 を介して、図示せず表示部に表示される。ユーザ F は、表示された U C P および P T の内容を参照して、図示せぬ操作部を操作し、U C P の 1 つの利用内容を選択する。これにより、入力制御部 6 8 は、操作部から入力された、ユーザ F の操作に対応する信号を S A M 6 2 に出力する。

この例の場合、レシーバ51の基準情報51の「利用ポイント情報」には、図33に示したように、コンテンツプロバイダ2-1のコンテンツ利用ポイントが222ポイントであるとされてる。すなわち、この基準情報51によれば、コンテンツAに対応して設定されたUCPA、Bのうち、「利用条件10」の「ユーザ条件10」が”200ポイント以上”とされている、UCPAが選択される。また、基準情報51の「決済ユーザ情報」には、ユーザFは男性とされているので、PTA-1（図20A）の「価格条件10」に設定された条件を満たす。その結果、UCPAに対応して作成されたPTA-1、PTA-2のうち、PTA-1が選択される。結局、UCPAおよびPTA-1の内容が、表示部に表示される。また、この例の場合、これにより、ユーザFが、UCPAの利用内容11（PTA-1の価格内容11）を選択したものとする。

ステップS245において、レシーバ51のSAM62の課金処理モジュール72は、ステップS244で選択された、UCPAの「利用内容11」の内容（PTA-1の「価格内容11」の内容）に基づいて、UCSA（図28）および課金情報A（図30）を作成する。すなわち、この場合、コンテンツAは、料金が2000円で買い取り再生される。

ステップS246において、サービスプロバイダセキュアコンテナ（図24）に含まれる、コンテンツA（コンテンツ鍵KcoAで暗号化されている）、UCPA、PT-1、A-2、およびコンテンツプロバイダ2の署名が取り出され、HDD52に出力され、記憶される。ステップS247において、復号／暗号化ユニット74の復号ユニット91は、サービスプロバイダセキュアコンテナに含まれるコンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）を、記憶モジュール73に記憶されている配送用鍵Kdで復号する。

ステップS248において、復号／暗号化ユニット74の暗号化ユニット93は、ステップS247で復号されたコンテンツ鍵KcoAを、記憶モジュール73に記憶されている保存用鍵Ksaveで暗号化する。

ステップS249において、SAM62のデータ検査モジュール75は、ステ

ップS 2 4 8で保存用鍵K s a v eで暗号化されたコンテンツ鍵K c o A、およびステップS 2 4 5で作成されたU C S Aが対応して記憶される、外部記憶部6 3の利用情報記憶部6 3 A（図2 9）の空き領域を有するブロックB Pを検出する。この例の場合、利用情報記憶部6 3 AのブロックB P - 1が検出される。なお、図2 9の利用情報記憶部6 3 Aにおいて、そのブロックB P - 1の利用情報用メモリ領域R P - 3にコンテンツ鍵K c o AおよびU C S Aが記憶されているように示されているが、この例の場合、この時点において、それらは記憶されておらず、ブロックB P - 1の利用情報用メモリ領域R P - 3は、空いており、所定の初期情報が記憶されているものとする。

ステップS 2 5 0において、レシーバ5 1のデータ検査モジュール7 5は、ステップS 2 4 9で検出したブロックB P - 1のデータ（利用情報用メモリ領域R P - 1乃至R P - Nに記憶されている全てのデータ）にハッシュ関数を適用して、ハッシュ値を得る。次に、ステップS 2 5 1において、データ検査モジュール7 5は、ステップS 2 5 0で得られたハッシュ値と、記憶モジュール7 3に記憶されているブロックB P - 1に対応する検査値H P - 1（図3 1）とを比較し、一致するか否かを判定し、一致すると判定した場合、そのブロックB P - 1のデータは改竄されていないので、ステップS 2 5 2に進む。

ステップS 2 5 2において、レシーバ5 1のS A M 6 2は、利用情報（ステップS 2 4 8で、保存用鍵K s a v eで暗号化されたコンテンツ鍵K c o A、およびステップS 2 4 5で作成されたU C S A（図2 8））を、図2 9に示すように、利用情報記憶部6 3 A（外部記憶部6 3）のブロックB P - 1の利用情報用メモリ領域R P - 3に記憶させる。

ステップS 2 5 3において、レシーバ5 1のデータ検査モジュール7 5は、ステップS 2 5 2で利用情報が記憶された利用情報用メモリ領域R P - 3が属する、利用情報記憶部6 3 AのブロックB P - 1のデータにハッシュ関数を適用し、ハッシュ値を算出し、ステップS 2 5 4において、記憶モジュール7 3に記憶されている検査値H P - 1に上書きする。ステップS 2 5 5において、課金処理モ

ジュール 7 2 は、ステップ S 2 4 5 で作成した課金情報 A を記憶モジュール 7 3 に記憶させ、処理は終了する。

ステップ S 2 5 1 において、算出されたハッシュ値と検査値 H P - 1 とが一致しないと判定された場合、ブロック B P - 1 のデータは改竄されているので、手続きは、ステップ S 2 5 6 に進み、データ検査モジュール 7 5 は、外部記憶部 6 3 の利用情報記憶部 6 3 A の全てのブロック B P を調べたか否かを判定し、外部記憶部 6 3 の全てのブロック B P を調べていないと判定した場合、ステップ S 2 5 7 に進み、利用情報記憶部 6 3 A の、調べていない（空きを有する他の）ブロック B P を検索し、ステップ S 2 5 0 に戻り、それ以降の処理が実行される。

ステップ S 2 5 6 において、外部記憶部 6 3 の利用情報記憶部 6 3 A の全てのブロック B P が調べられたと判定された場合、利用情報を記憶できるブロック B P（利用情報用メモリ領域 R P）は存在しないので、処理は終了する。

このように、サービスプロバイダセキュアコンテナが、レシーバ 5 1 により受信されると、処理は終了し、図 3 8 のステップ S 1 5 に進む。

（6 - 5）コンテンツの再生処理

ステップ S 1 5 において、供給されたコンテンツ A が、レシーバ 5 1 において利用される。なお、この例の場合、図 4 5 のステップ S 2 2 4 で選択された U C P A の利用内容 1 1 によれば、コンテンツ A は、再生して利用される。そこで、ここでは、コンテンツ A の再生処理について説明する。この再生処理の詳細は、図 4 6 のフローチャートに示されている。

ステップ S 2 6 1 において、レシーバ 5 1 のデータ検査モジュール 7 5 は、図 4 5 のステップ S 2 5 2 で、コンテンツ鍵 K c o A（保存用鍵 K s a v e で暗号化されている）および U C S A が記憶された利用情報用メモリ領域 R P - 3 が属する、外部記憶部 6 3 の利用情報記憶部 6 3 A のブロック B P - 1 のデータにハッシュ関数を適用してハッシュ値を算出する。

ステップ S 2 6 2 において、レシーバ 5 1 のデータ検査モジュール 7 5 は、ステップ S 2 6 1 において算出したハッシュ値が、図 4 5 のステップ S 2 5 3 で算

出し、ステップS 2 5 4で記憶モジュール7 3に記憶させたハッシュ値（検査値HP-1）と一致するか否かを判定し、一致すると判定した場合、ブロックBP-1のデータは改竄されていないので、ステップS 2 6 3に進む。

ステップS 2 6 3において、UCSA（図28）の「利用内容」の「パラメータ」に示されている情報に基づいて、コンテンツAが利用可能か否かが判定される。例えば、「利用内容」の「形式」が、「期間制限再生」とされているUCSにおいては、その「パラメータ」には、その開始期間（時刻）と終了期間（時刻）が記憶されているので、この場合、現在の時刻が、その範囲内にあるか否かが判定される。すなわち、現在時刻が、その範囲内にあるとき、そのコンテンツの利用が可能であると判定され、範囲外にあるとき、利用不可と判定される。また、「利用内容」の「形式」が、所定の回数に限って再生（複製）する利用形式とされているUCSにおいては、その「パラメータ」には、残された利用可能回数が記憶されている。この場合、「パラメータ」に記憶されている利用可能回数が0回でないとき、対応するコンテンツの利用が可能であると判定され、一方、利用可能回数が0回であるとき、利用不可と判定される。

なお、UCSAの「利用内容」の「形式」は、「買い取り再生」とされているので、この場合、コンテンツAは、買い取られ、制限なしに再生される。すなわち、UCSAの「利用内容」の「パラメータ」には、コンテンツが利用可能であることを示す情報が設定されている。そのため、この例の場合では、ステップS 2 6 3において、コンテンツAが利用可能であると判定され、ステップS 2 6 4に進む。

ステップS 2 6 4において、レシーバ51の課金モジュール72は、UCSAを更新する。UCSAには、更新すべき情報は含まれていないが、例えば、「利用内容」の「形式」が所定の回数に限って再生する利用形式とされている場合、その「パラメータ」に記憶されている、再生可能回数が1つだけデクリメントされる。

次に、ステップS 2 6 5において、レシーバ51のSAM62は、ステップS

264で更新されたUCSA（この例の場合には、実際は、更新されていない）を、外部記憶部63の利用情報記憶部63AのブロックBP-1の利用情報用メモリ領域RP-3に記憶させる。ステップS266において、データ検査モジュール75は、ステップS265でUCSAが記憶された、外部記憶部63の利用情報記憶部63AのブロックBP-1のデータにハッシュ関数を適用して、ハッシュ値を算出し、記憶モジュール73に記憶されている検査値HP-1に上書きする。

ステップS267において、SAM62の相互認証モジュール71と、伸張部64の相互認証モジュール101は、相互認証し、SAM62および伸張部64は、一時鍵Ktempを共有する。この認証処理は、図40乃至図42を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数R1、R2、R3、またはその組み合わせが、一時鍵Ktempとして用いられる。

ステップS268において、復号／暗号化モジュール74の復号ユニット91は、図45のステップS252で外部記憶部63の利用情報記憶部63AのブロックBP-1（利用情報用メモリ領域RP-3）に記憶されたコンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）を、記憶モジュール73に記憶された保存用鍵Ksaveで復号する。

次に、ステップS269において、復号／暗号化モジュール74の暗号化ユニット93は、復号されたコンテンツ鍵KcoAを一時鍵Ktempで暗号化する。ステップS270において、SAM62は、一時鍵Ktempで暗号化されたコンテンツ鍵KcoAを伸張部64に送信する。

ステップS271において、伸張部64の復号モジュール102は、コンテンツ鍵KcoAを一時鍵Ktempで復号する。ステップS272において、伸張部64は、インタフェース66を介して、HDD52に記録されたコンテンツA（コンテンツ鍵Kcoで暗号化されている）を受け取る。ステップS273において、伸張部64の復号モジュール103は、コンテンツA（コンテンツ鍵Kc

oで暗号化されている)をコンテンツ鍵K c o Aで復号する。

ステップS 2 7 4において、伸張部6 4の伸張モジュール1 0 4は、復号されたコンテンツAをA T R A C 2などの所定の方式で伸張する。ステップS 2 7 5において、伸張部6 4のウォータマーク付加モジュール1 0 5は、伸張されたコンテンツAにレシーバ5 1を特定する所定のウォータマーク(電子透かし)を挿入する。ステップS 2 7 6において、コンテンツAは、図示せぬスピーカなどに出力され、処理は終了する。

ステップS 2 6 2において、ステップS 2 6 1において算出されたハッシュ値が、レシーバ5 1の記憶モジュール7 3に記憶されたハッシュ値と一致しないと判定された場合、またはステップS 2 6 3において、コンテンツが利用不可と判定された場合、ステップS 2 7 7において、S A M 6 2は、表示制御部6 7を介して、図示せぬ表示部にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

このようにして、レシーバ5 1において、コンテンツAが再生(利用)されたとき、処理は終了し、図3 8の処理も終了する。

(6-6) 決済処理

次に、レシーバ5 1の課金が決済される場合の処理手順を、図4 7のフローチャートを参照して説明する。なお、この処理は、計上された課金が所定の上限額(正式登録時の上限額または仮登録時の上限額)を越えた場合、または配送用鍵K dのバージョンが古くなり、例えば、図4 5のステップS 2 4 7で、コンテンツ鍵K c o(配送用鍵K dで暗号化されている)を復号することができなくなった場合(サービスプロバイダセキュアコンテナを受信することができなくなった場合)に開始される。

ステップS 3 0 1において、レシーバ5 1とEMDサービスセンタ1との相互認証が行われる。この相互認証は、図4 0乃至図4 2を参照して説明した場合と同様の処理であるので、その説明は省略する。

次に、ステップS 3 0 2において、レシーバ5 1のS A M 6 2は、EMDサー

ビスセンタ1のユーザ管理部18（図3）に証明書を送信する。ステップS303において、レシーバ51のSAM62は、記憶モジュール73に記憶されている課金情報を、ステップS301で、EMDサービスセンタ1と共有した一時鍵Ktempで暗号化し、配送用鍵Kdのバージョン、HDD52に記憶されてる、対応するUCPとPT、並びに登録リストとともに、EMDサービスセンタ1に送信する。

ステップS304において、EMDサービスセンタ1のユーザ管理部18は、ステップS303で、レシーバ51から送信された情報を受信し、復号した後、EMDサービスセンタ1のユーザ管理部18が、登録リストの「状態フラグ」に”停止”が設定されるべき不正行為がレシーバ51において存在するか否かを確認する。

ステップS305において、EMDサービスセンタ1の課金請求部19は、ステップS303で受信された課金情報を解析し、ユーザ（例えば、ユーザF）の支払い金額を算出する処理等を行う。次に、ステップS306において、ユーザ管理部18は、ステップS305における処理により、決済が成功したか否かを確認する。

次に、ステップS307において、EMDサービスセンタ1のユーザ管理部18は、ステップS304における確認結果、およびステップS306における確認結果に基づいて、レシーバ51の登録条件を設定し、それに署名を付して、レシーバ51の登録リストを作成する。

例えば、ステップS304で、不正行為が確認された場合、「状態フラグ」には”停止”が設定され、この場合、今後、全ての処理が停止される。すなわち、EMDシステムからのサービスを一切受けることができなくなる。また、ステップS306で、決済が成功しなかったことが確認された場合、「状態フラグ」には”制限あり”が設定され、この場合、すでに購入したコンテンツを再生する処理は可能とされるが、新たにコンテンツを購入する処理は実行できなくなる。

次に、ステップS308に進み、EMDサービスセンタ1のユーザ管理部18

は、最新バージョンの配送用鍵K d（3ヶ月分の最新バージョンの配送用鍵K d）およびステップS 3 0 7で作成された登録リストを、一時鍵K t e m pで暗号化し、レシーバ5 1に送信する。なお、登録リストには、署名が付されているので、暗号化しなくてもよい。

ステップS 3 0 9において、レシーバ5 1のS A M 6 2は、EMDサービスセンタ1から送信された配送用鍵K dおよび登録リスト情報を、通信部6 1を介して受信し、復号した後、配送用鍵K dを記憶モジュール7 3に記憶させ、登録リストをHDD 5 2に記憶させる。このとき、記憶モジュール7 3に記憶されていた課金情報は消去され、登録リストおよび配送用鍵K dが更新される。

（6－7）管理移動の設定

次に、レシーバ5 1からレシーバ2 0 1に、コンテンツAが管理移動される場合の処理手順を、図4 8のフローチャートを参照して説明する。

ステップS 4 0 1において、レシーバ5 1とレシーバ2 0 1との間で、相互認証が行われる。この相互認証は、図4 0乃至図4 2を参照して説明した同様であるので、その説明は省略する。

次に、ステップS 4 0 2において、レシーバ5 1（管理移動元の機器）のS A M 6 2およびレシーバ2 0 1（管理移動先の機器のS A M）のS A M 2 1 2のそれぞれは、各自が保持する登録リストを参照し、コンテンツの管理移動が可能であるか否かを確認する。具体的には、管理移動元の機器のS A M（レシーバ5 1のS A M 6 2）は、自分の登録リストに、管理移動先の機器（レシーバ2 0 1）の登録条件が設定されているか否かを確認し、それが設定されている場合、コンテンツの管理移動が可能であると判定する。同様に、管理移動先の機器のS A M（レシーバ2 0 1のS A M 2 1 2）も、自分の登録リストに、管理移動元の機器（レシーバ5 1）の登録条件が設定されているか否かを確認し、それが設定されている場合、コンテンツの管理移動が可能であると判定する。いずれか一方においても、コンテンツの管理移動が可能でないと判定された場合、処理は終了するが、この例の場合、それぞれの登録条件は、それぞれの登録リストに設定されて

いるので、両者において、コンテンツの管理移動が可能であると判定され、ステップS403に進む。

次に、ステップS403において、レシーバ201のデータ検査モジュール225は、後述するステップS414で受信する移動情報（コンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）、コンテンツAのID、およびSAM62のID）を記憶する、外部記憶部213の移動情報記憶部213A（図36）のブロックBMを検出する。この例の場合、ステップS403において、ブロックBM-1が検出される。なお、図36の利用情報記憶部213Aにおいて、そのブロックBM-1の移動情報用メモリ領域RM-1には、コンテンツ鍵KcoA、コンテンツAのID、およびSAM62のIDが記憶されているように示されているが、この例の場合、この時点において、その移動情報用メモリ領域RM-1は、空いているものとする。

ステップS404において、レシーバ201のデータ検査モジュール225は、ステップS403で検出したブロックBM-1のデータが改竄されているか否かを判定する。具体的には、データ検査モジュール225は、ブロックBM-1に記憶されているデータにハッシュ関数を適用してハッシュ値を算出する。そしてデータ検査モジュール225は、算出したハッシュ値と、記憶モジュール223に記憶される、ブロックBM-1に対応する検査値HM-1が一致するか否かを判定し、一致していると判定した場合、すなわち、ブロックBM-1が改竄されていない場合、ステップS405に進む。

ステップS405において、レシーバ201のSAM212は、コンテンツの管理移動が可能であることを示す信号を通信部215を介して、レシーバ51に送信する。

ステップS406において、レシーバ51が、レシーバ201から、コンテンツの管理移動が可能であることを示す信号を受信すると、レシーバ51のデータ検査モジュール75は、管理移動されるコンテンツAに対応するコンテンツ鍵KcoAが記憶されている、外部記憶部63の利用情報記憶部63A（図29）の

ブロック B P - 1 を検出する。

ステップ S 4 0 7 において、レシーバ 5 1 のデータ検査モジュール 7 5 は、ステップ S 4 0 6 で検出したブロック B P - 1 のデータが改竄されているか否かを判定する。具体的には、データ検査モジュール 7 5 は、ブロック B P - 1 に記憶されているデータの全てにハッシュ関数を適用してハッシュ値を算出する。そしてデータ検査モジュール 7 5 は、算出したハッシュ値が、記憶モジュール 7 3 に記憶されている、ブロック B P - 1 に対応する検査値 H P - 1 (図 4 5 のステップ S 2 5 3 で算出され、ステップ S 2 5 4 で記憶されたハッシュ値) と一致するか否かを判定し、一致すると判定した場合、すなわち、ブロック B P - 1 のデータが改竄されていない場合、ステップ S 4 0 8 に進む。

ステップ S 4 0 8 において、レシーバ 5 1 の S A M 6 2 は、ステップ S 4 0 6 で検出された、外部記憶部 6 3 の利用情報記憶部 6 3 のブロック B P - 1 (利用情報用メモリ領域 R P - 3) に記憶されている U C S A (図 2 8) の「利用内容」の「形式」を参照し、コンテンツの利用形式が” 買い取り再生” であるか否かを判定する。U C S A の場合のように、その「利用内容」の「形式」が、” 買い取り再生” とされているとき、コンテンツの利用形式が” 買い取り再生” であると判定され、ステップ S 4 0 9 に進む。

ステップ S 4 0 9 において、レシーバ 5 1 の S A M 6 2 は、U C S A の「利用内容」の「管理移動状態情報」に設定されている管理移動先の機器の I D が、自分自身の I D とされているか否か、すなわち、コンテンツが管理移動されているか否かを判定し、コンテンツが管理移動されていないと判定した場合、ステップ S 4 1 0 に進む。

ステップ S 4 1 0 において、レシーバ 5 1 の S A M 6 2 は、今回のコンテンツ A の管理移動先の機器であるレシーバ 2 0 1 の S A M 2 1 2 の I D を、U C S A の「利用内容」の「管理移動状態情報」に管理移動先の機器の I D として設定する。次に、ステップ S 4 1 1 において、レシーバ 5 1 のデータ検査モジュール 7 5 は、ステップ S 4 1 0 で、「利用内容」の「管理移動状態情報」の内容が変更

(管理移動先のIDが、SAM62のIDからSAM212のIDに変更)されたUCSAが記憶されているブロックBP-1のデータにハッシュ関数を適用しハッシュ値を算出し、それを、ステップS412において、記憶モジュール73に記憶されている、ブロックBP-1に対応するハッシュ値HP-1に上書きする。

次に、ステップS413において、レシーバ51のSAM62は、外部記憶部63の利用情報記憶部63AのブロックBP-1(利用情報用メモリ領域RP-3)に記憶されているコンテンツ鍵KcoA(保存用鍵Ksaveで暗号化されている)を保存用鍵Ksaveで復号し、ステップS401でレシーバ201と共有した一時鍵Ktempで暗号化した後、自分自身のID(SAM62のID)およびUCSAの「コンテンツのID」に設定されているコンテンツAのIDとともに、レシーバ201に送信する。なお、この処理が実行されるタイミングで、HDD52に記憶されているコンテンツAは、レシーバ201に送信される。

ステップS414において、レシーバ51から送信されてきたコンテンツ鍵KcoA(一時鍵Ktempで暗号化されている)、SAM62のID、およびコンテンツAのIDがレシーバ201により受信されると、ステップS415において、レシーバ201のSAM212は、受信されたコンテンツ鍵KcoA(一時鍵Ktempで暗号化されている)を一時鍵Ktempで復号した後、自分自身が保持している保存用鍵Ksaveで再度暗号化して、それを、同様にSAM62のID、コンテンツAのID、および自分自身のID(SAM212のID)とともに、ステップS403で検出した、外部記憶部213の移動情報記憶部213AのブロックBP-1の移動情報用メモリ領域RM-1に、図36で示したように記憶させる。

次に、ステップS416において、レシーバ201のSAM212は、ステップS415で移動情報が記憶された移動情報記憶部213AのブロックBM-1のデータにハッシュ関数を適用してハッシュ値を算出し、記憶モジュール223

に記憶されている検査値HM-1に上書きする。

ステップS417において、レシーバ51から供給されたコンテンツAがHD202に記憶される。

ステップS404で外部記憶部213の移動情報記憶部213AのブロックBM-1のデータが、またはステップS407で外部記憶部63の利用情報記憶部63AのブロックBP-1のデータが改竄されていると判定された場合、処理は終了する。すなわち、移動情報が記憶されるメモリ領域がまたは、利用情報が改竄されている場合（正確には、改竄されている恐れがある場合）、コンテンツの管理移動は行われぬ。

ステップS407で、コンテンツAの利用形式が”買い取り”ではないと判定された場合、またはステップS408で、コンテンツAが管理移動されていると判定された場合も、処理は終了する。すなわち、コンテンツを買い取って再生する利用形式においてのみ、コンテンツの管理移動が行われる（許可されている）。また、コンテンツが管理移動されている間は、さらに、そのコンテンツを管理移動することはできない（許可されていない）。

（6-8）管理移動の解除

次に、上述した処理により、レシーバ201にコンテンツAが管理移動されている状態において、今度は、レシーバ51が、コンテンツAを戻す（管理移動を解除する）場合の処理手順を、図49のフローチャートを参照して説明する。

ステップS431において、レシーバ51とレシーバ201との間で、相互認証が行われる。この相互認証は、図40乃至図42を参照して説明した場合と同様であるので、その説明は省略する。次に、ステップS432において、レシーバ51（管理移動元の機器）のSAM62およびレシーバ201（管理移動先の機器のSAM）のSAM212のそれぞれは、各自が保持する登録リストを参照し、管理移動の解除が可能であることを確認する。なお、ここでの具体的な処理は、図48のステップS402における場合と同様であるので、その説明は省略する。

ステップS 4 3 3において、レシーバ5 1のデータ検査モジュール7 5は、管理移動されているコンテンツA（コンテンツ鍵K c o Aで暗号化されている）に対応するコンテンツ鍵K c o Aが記憶されている外部記憶部6 3の利用情報記憶部6 3 A（図2 9）のブロックB Pを検出する。この例の場合、ブロックB P－1が検出される。

次に、ステップS 4 3 4において、レシーバ5 1のデータ検査モジュール7 5は、ステップS 4 3 3で検出したブロックB P－1のデータが改竄されているか否かを判定する。ここでの具体的な処理は、図4 8のステップS 4 0 7における場合と同様であるので、その説明は省略する。

ステップS 4 3 4で、外部記憶部6 3の利用情報記憶部6 3 AのブロックB P－1のデータが改竄されていないと判定された場合、ステップS 4 3 5に進み、レシーバ5 1のS A M 6 2は、外部記憶部6 3の利用情報記憶部6 3 AのブロックB P－1に記憶されているU C S A（図2 8）から、コンテンツAのI DおよびS A M 6 2のI Dを読み出し、それらを、管理移動の解除を要求する所定の信号（以下、管理移動解除要求信号と称する）とともに、レシーバ2 0 1に送信する。

ステップS 4 3 6において、レシーバ5 1から送信されてきた、コンテンツAのI D、S A M 6 2のI D、および管理移動解除要求信号が受信されると、ステップS 4 3 7において、レシーバ2 0 1のS A M 2 1 2は、受信されたコンテンツAのI Dが記憶されている、外部記憶部2 1 3の移動情報記憶部2 1 3 AのブロックB Mを検出する。この例の場合、ブロックB M－1が検出される。

ステップS 4 3 8において、レシーバ2 0 1のS A M 2 1 2は、外部記憶部2 1 3の移動情報記憶部2 1 3 AのブロックB M－1（移動情報用メモリ領域R M－1）に、ステップS 4 3 6で受信されたS A M 6 2のI Dが記憶されているか否かを判定し、記憶されていると判定した場合、ステップS 4 3 9に進む。この例の場合、ブロックB M－1の移動情報用メモリ領域R M－1には、S A M 6 2のI Dが記憶されているので、ステップS 4 3 9に進む。

ステップS 4 3 9において、レシーバ2 0 1のSAM 2 1 2は、SAM 6 2のIDが記憶されてるブロックBM-1が改竄されているか否かを判定する。ここでの具体的な処理は、図4 8のステップS 4 0 4における場合と同様であるので、その説明は省略する。ステップS 4 3 9において、ブロックBM-1が改竄されていないと判定された場合、ステップS 4 4 0に進む。

ステップS 4 4 0において、レシーバ2 0 1のSAM 2 1 2は、外部記憶部2 1 3の移動情報記憶部2 1 3 AのブロックBM-1（移動情報用メモリ領域RM-1）に、ステップS 4 3 6で受信されたコンテンツのIDが記憶されているか否かを判定し、記憶されていると判定した場合、ステップS 4 4 1に進む。この例の場合、ブロックBM-1の移動情報用メモリ領域RM-1には、コンテンツAのIDが記憶されているので、ステップS 4 4 1に進む。

ステップS 4 4 1において、レシーバ2 0 1のSAM 2 1 2は、外部記憶部2 1 3の移動情報記憶部2 1 3 AのブロックBM-1（移動情報用メモリ領域RM-1）に記憶されている移動情報を削除する。これにより、ブロックBM-1の移動情報用メモリ領域RM-1には、所定の初期情報が記憶される。なお、この処理が実行されるタイミングで、HDD 2 0 2に記憶されているコンテンツAも削除される。

次に、ステップS 4 4 2において、レシーバ2 0 1のデータ検査モジュール2 2 5は、ステップS 4 4 1で移動情報が削除された移動情報用メモリ領域RM-1が属するブロックBM-1のデータにハッシュ関数を適用してハッシュ値を算出し、それを、記憶モジュール2 2 3に記憶されている、ブロックBM-1に対応するハッシュ値HM-1に上書きする。

ステップS 4 4 3において、レシーバ2 0 1のSAM 2 1 2は、コンテンツの管理移動が解除されたことを示す信号（以下、管理移動解除信号と称する）を、レシーバ5 1に送信する。

ステップS 4 4 4において、レシーバ2 0 1からの管理移動解除信号が受信されると、レシーバ5 1のSAM 6 2は、自分自身のIDを、UCSAの「利用内容」

の「管理移動状態情報」に、管理移動先の機器のIDとして記憶させる（管理移動元の機器のIDは、SAM62のIDとされている）。

次に、ステップS445において、レシーバ51のデータ検査モジュール75は、ステップS444で、「利用内容」の管理移動状態情報の内容が変更（管理移動先のIDが、SAM212のIDからSAM62のIDに変更）されたUCSAが記憶されているブロックBP-1のデータにハッシュ関数を適用してハッシュ値を算出し、それを、ステップS446において、記憶モジュール73に記憶されている、ブロックBP-1に対応する検査値HP-1に上書きする。

以上のようにして、コンテンツの管理移動が解除されるとき、管理移動先の機器である、レシーバ201から移動情報が削除されるようにしたので、レシーバ201においてコンテンツAは利用されないようになる。またこのとき、UCSAの「利用内容」の「管理移動状態情報」に、管理移動元の機器のSAMのID（レシーバ51のSAM62）のIDが、管理移動先の機器のIDとしても設定されるようにしたので、レシーバ51は、コンテンツAの管理移動を行うことができるようになる。

なお、以上においては、コンテンツの利用形式が”買い取り再生”である場合にのみ管理移動が可能となる場合を例として説明したが、利用形式が”期間制限再生”である場合においても管理移動が可能となるようにすることもできる。

また、以上においては、管理移動が解除される場合、レシーバ51がレシーバ201に管理移動解除要求信号を送信する場合（レシーバ51が管理移動の解除を要求する場合）を例として説明したが、レシーバ201が管理移動の解除を要求することもできる。

さらに、以上においては、SAM62の公開鍵K_{pu}およびSAM62の証明書がレシーバ51の記憶モジュール73が記憶されているものとしたが、HDD52に記憶させておくこともできる。同様に、SAM212の公開鍵K_{pu}およびSAM212の証明書も、HDD202に記憶させておくこともできる。

なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動

画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であればMPEG (Moving Picture Experts Group) などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

また、共通鍵暗号は、ブロック暗号であるDESを使用して説明したが、NTT (商標) が提案するFEAL、IDEA (International Data Encryption Algorithm)、または1ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

さらに、コンテンツおよびコンテンツ鍵K_{co}の暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

上述した本発明の実施の形態のレシーバにおいては、移動状態情報が、価値情報の移動が行われていないことを示しているとき、価値情報、および価値情報を復号するのに必要な鍵を含む移動情報が他の情報処理装置に供給されたとき、移動状態情報の内容を、価値情報の移動が行われていることを示すものに変更し、所定の制御信号に対する応答信号が受信されたとき、移動状態情報の内容を、価値情報の移動が行われていないことを示すものに変更するようにしたので、著作権の保護を確保しながら、価値情報の移動を行うことができる。

また、本発明の実施の形態のレシーバにおいては、他の情報処理装置から供給される価値情報、および価値情報を復号するのに必要な鍵を含む移動情報を受信し、所定の制御信号を受信したとき、記憶された移動情報を削除するようにしたので、著作権の保護を確保しながら、移動された価値情報を利用することができ

る。

産業上の利用の可能性

本発明は、音楽データ、動画像データ、静止画像データ、文書データ、プログラムデータなどの情報を暗号化し、配信する情報処理システムに適応できる。

請 求 の 範 囲

1. 他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置において、

上記価値情報を復号するのに必要な鍵、上記価値情報の使用条件、および上記価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶手段と、

上記記憶手段により記憶されている上記利用情報に含まれる上記使用条件が所定の条件で、かつ、上記利用情報に含まれる上記移動状態情報が、上記価値情報の移動が行われていないことを示しているとき、上記価値情報、および上記利用情報に含まれる上記鍵を含む所定の移動情報を上記他の情報処理装置に供給する供給手段と、

上記供給手段により、上記価値情報、および上記移動情報が上記他の情報処理装置に供給されたとき、上記移動状態情報の内容を、上記価値情報の移動が行われていることを示すものに変更する第1の変更手段と、

上記記憶手段により記憶されている上記利用情報に含まれる上記移動状態情報が、上記価値情報の移動が行われていることを示しており、上記情報処理装置への上記価値情報の移動を解除するとき、上記他の情報処理装置に所定の制御信号を送信する送信手段と、

上記他の情報処理装置から、上記送信手段により送信された上記制御信号に対する応答信号を受信したとき、上記移動状態情報の内容を、上記価値情報の移動が行われていないことを示すものに変更する第2の変更手段と

を具備する情報処理装置。

2. 上記記憶手段は、所定のメモリ領域に分割されている複数のブロックにより構成され、上記利用情報を、上記所定のメモリ領域に記憶し、

上記記憶手段を構成する上記ブロックに記憶されている複数の上記利用情報の

全体にハッシュ関数を適用し、ハッシュ値を算出する算出手段と、

ハッシュ値を記憶するハッシュ値記憶手段と、

上記算出手段により算出された上記ハッシュ値と、上記ハッシュ値記憶手段に記憶されている所定のハッシュ値を比較し、比較結果に基づいて、上記記憶手段が改竄されたか否かを判定する判定手段と、

上記判定手段による判定結果に基づいて、上記供給手段による供給を制御する制御手段と

をさらに具備する請求の範囲第1項に記載の情報処理装置。

3. 他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置の情報処理方法において、

上記価値情報を復号するのに必要な鍵、上記価値情報の使用条件、および上記価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶ステップと、

上記記憶ステップで記憶された上記利用情報に含まれる上記使用条件が所定の条件で、かつ、上記利用情報に含まれる上記移動状態情報が、上記価値情報の移動が行われていないことを示しているとき、上記価値情報、および上記利用情報に含まれる上記鍵を含む所定の移動情報を上記他の情報処理装置に供給する供給ステップと、

上記供給ステップで、上記価値情報、および上記移動情報が上記他の情報処理装置に供給されたとき、上記移動状態情報の内容を、上記価値情報の移動が行われていることを示すものに変更する第1の変更ステップと、

上記記憶ステップで記憶されている上記利用情報に含まれる上記移動状態情報が、上記価値情報の移動が行われていることを示しており、上記情報処理装置への上記価値情報の移動を解除するとき、上記他の情報処理装置に所定の制御信号を送信する送信ステップと、

上記他の情報処理装置から、上記送信ステップで送信された上記制御信号に対

する応答信号を受信したとき、上記移動状態情報の内容を、上記価値情報の移動が行われていないことを示すものに変更する第2の変更ステップと
を具備する情報処理方法。

4. 他の情報処理装置に接続され、暗号化された価値情報を復号し、利用する情報処理装置に、

上記価値情報を復号するのに必要な鍵、上記価値情報の使用条件、および上記価値情報の移動が行われているか否かを示す移動状態情報を含む利用情報を記憶する記憶ステップと、

上記記憶ステップで記憶された上記利用情報に含まれる上記使用条件が所定の条件で、かつ、上記利用情報に含まれる上記移動状態情報が、上記価値情報の移動が行われていないことを示しているとき、上記価値情報、および上記利用情報に含まれる上記鍵を含む所定の移動情報を上記他の情報処理装置に供給する供給ステップと、

上記供給ステップで、上記価値情報、および上記移動情報が上記他の情報処理装置に供給されたとき、上記移動状態情報の内容を、上記価値情報の移動が行われていることを示すものに変更する第1の変更ステップと、

上記記憶ステップで記憶されている上記利用情報に含まれる上記移動状態情報が、上記価値情報の移動が行われていることを示しており、上記他の情報処理装置への上記価値情報の移動を解除するとき、上記他の情報処理装置に所定の制御信号を送信する送信ステップと、

上記他の情報処理装置から、上記送信ステップで送信された上記制御信号に対する応答信号を受信したとき、上記移動状態情報の内容を、上記価値情報の移動が行われていないことを示すものに変更する第2の変更ステップと

を具備する処理を実行させるコンピュータが読み取り可能なプログラムを提供する提供媒体。

5. 他の情報処理装置に接続され、暗号化された上記価値情報を復号し、利用する情報処理装置において、

上記他の情報処理装置から供給される上記価値情報、および上記価値情報を復号するのに必要な鍵を含む移動情報を受信する受信手段と、

上記受信手段により受信された上記移動情報を記憶する記憶手段と、

上記他の情報処理装置から、所定の制御信号を受信したとき、上記記憶手段に記憶されている上記移動情報を削除する削除手段と、

上記削除手段により、上記移動情報が削除されたとき、所定の応答信号を送信する送信手段と

を具備する情報処理装置。

6. 上記記憶手段は、所定のメモリ領域に分割されている複数のブロックにより構成され、上記移動情報を、上記所定のメモリ領域に記憶するし、

上記記憶手段の上記ブロックごとに記憶されている複数の上記移動情報の全体にハッシュ関数を適用し、ハッシュ値を算出する算出手段と、

ハッシュ値を記憶するハッシュ値記憶手段と、

上記算出手段により算出された上記ハッシュ値と、上記ハッシュ値記憶手段に記憶されている所定のハッシュ値を比較し、比較結果に基づいて、上記記憶手段が改竄されたか否かを判定する判定手段と、

上記判定手段による判定結果に基づいて、上記受信手段による受信を制御する制御手段と

をさらに具備する請求の範囲第5項に記載の情報処理装置。

7. 他の情報処理装置に接続され、暗号化された上記価値情報を復号し、利用する情報処理装置の情報処理方法において、

上記他の情報処理装置から供給される上記価値情報、および上記価値情報を復号するのに必要な鍵を含む移動情報を受信する受信ステップと、

上記受信ステップで受信された上記移動情報を記憶する記憶ステップと、
上記他の情報処理装置から、所定の制御信号を受信したとき、上記記憶ステップで記憶された上記移動情報を削除する削除ステップと、
上記削除ステップで、上記移動情報が削除されたとき、所定の応答信号を送信する送信ステップと
を具備する情報処理方法。

8. 他の情報処理装置に接続され、暗号化された上記価値情報を復号し、利用する情報処理装置に、

上記他の情報処理装置から供給される上記価値情報、および上記価値情報を復号するのに必要な鍵を含む移動情報を受信する受信ステップと、

上記受信ステップで受信された上記移動情報を記憶する記憶ステップと、

上記他の情報処理装置から、所定の制御信号を受信したとき、上記記憶ステップで記憶された上記移動情報を削除する削除ステップと、

上記削除ステップで、上記移動情報が削除されたとき、所定の応答信号を送信する送信ステップと

を具備する処理を実行させるコンピュータが読み取り可能なプログラムを提供する提供媒体。

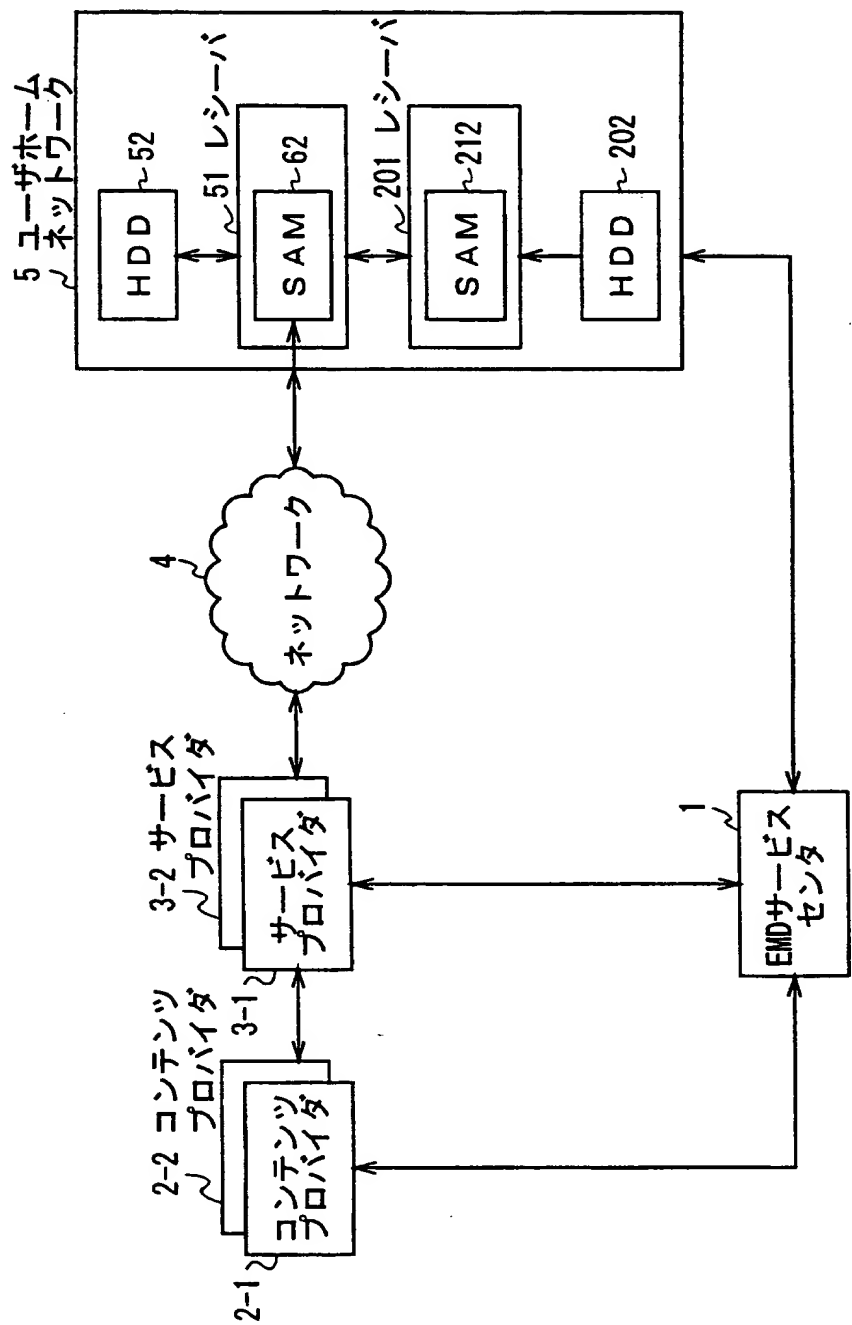


図 1

This Page Blank (uspto)

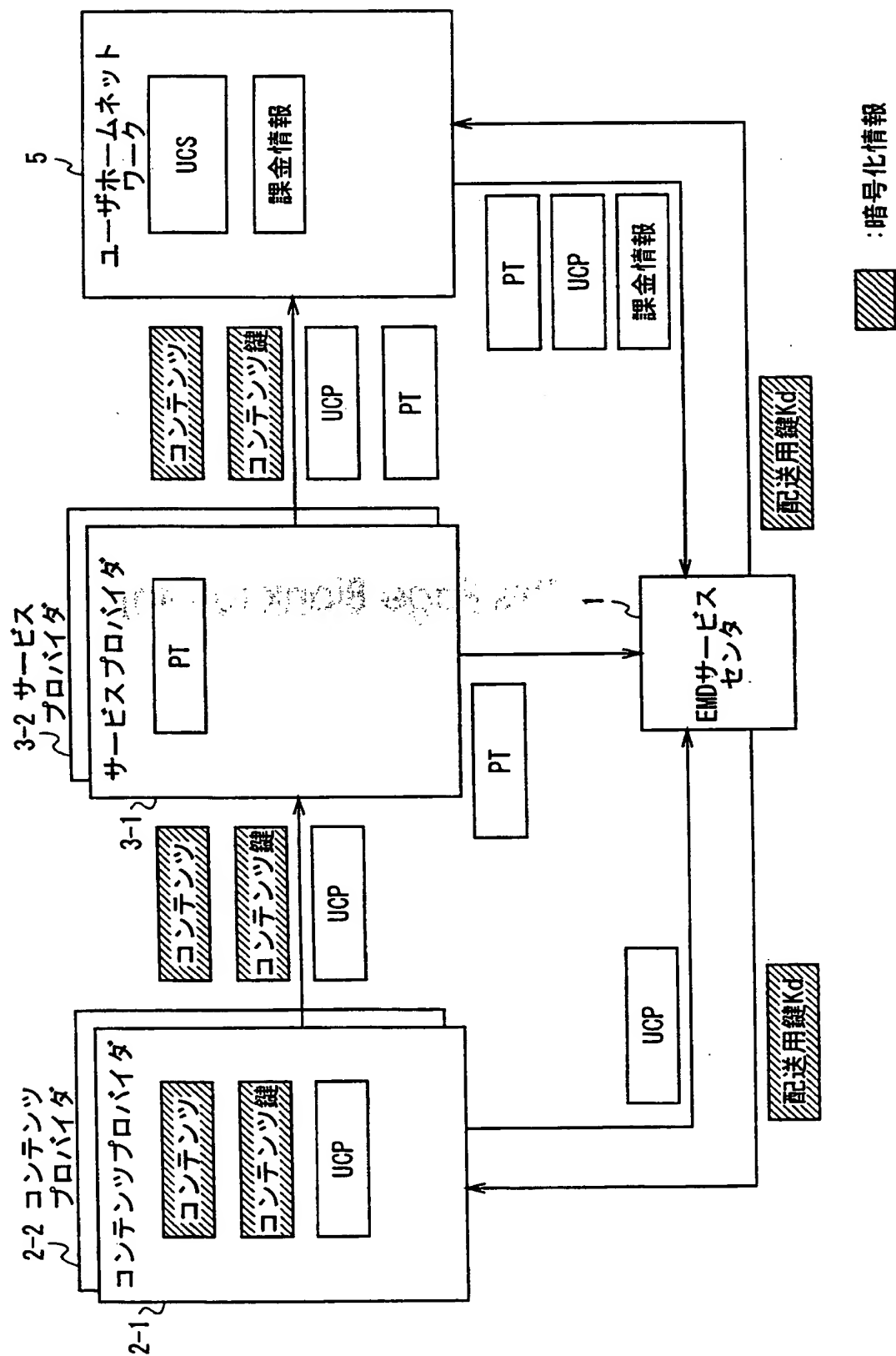
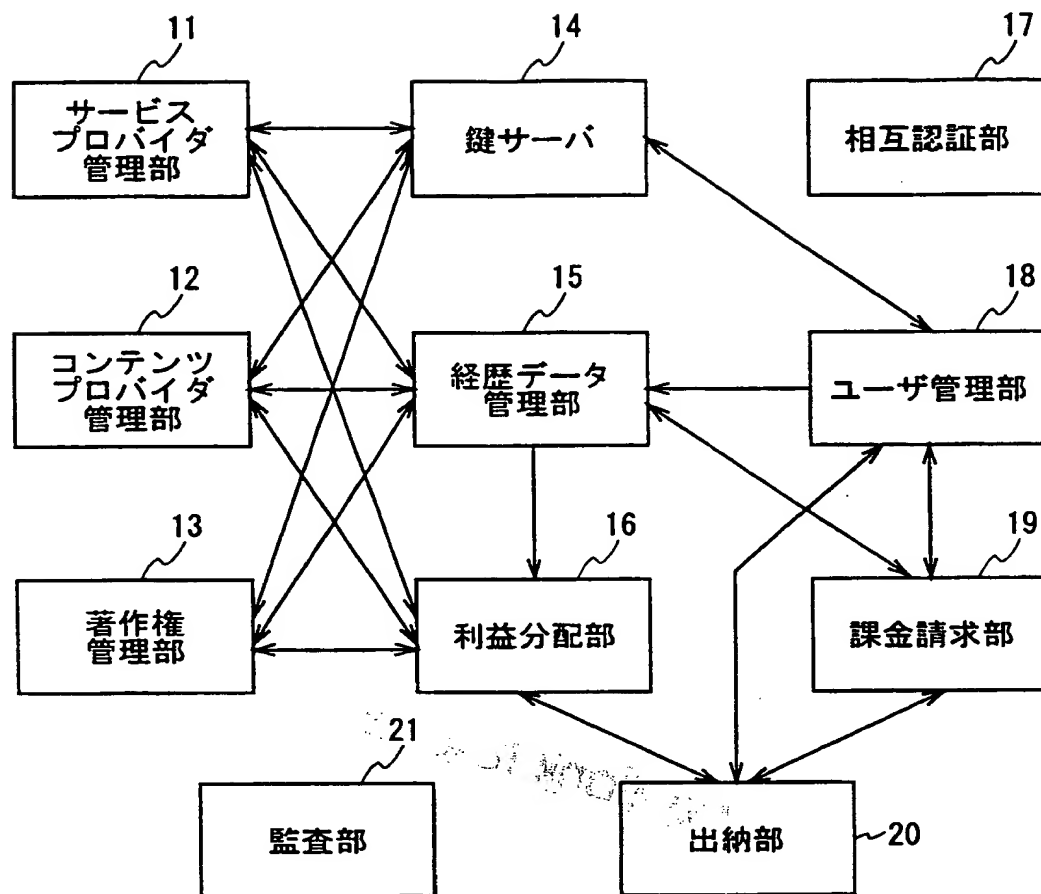


図 2

This Page Blank (uspto)



EMDサービスセンタ 1

図 3

This Page Blank (uspto)

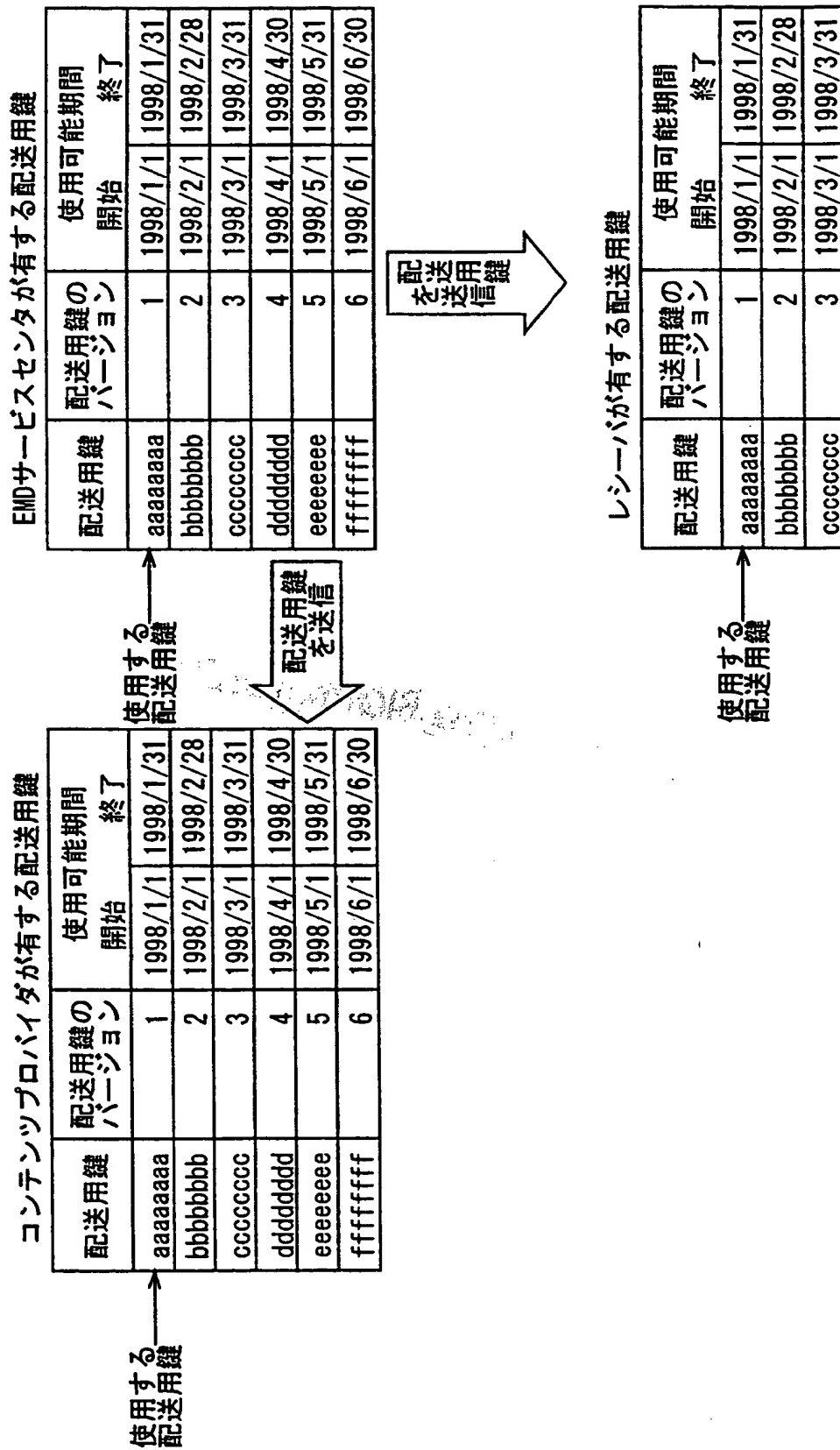


図 4

This Page Blank (uspto)

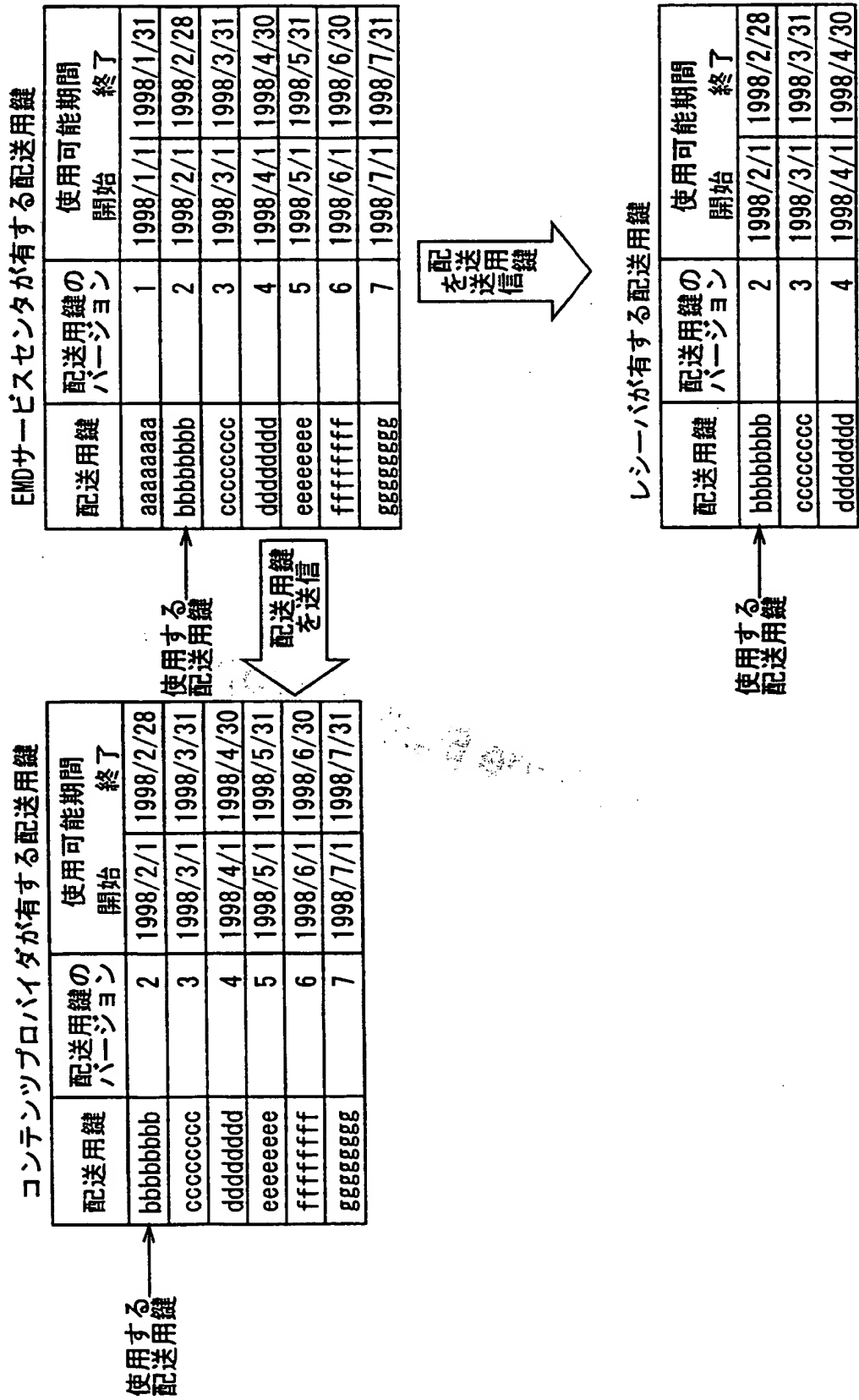


図 5

This Page Blank (uspto)

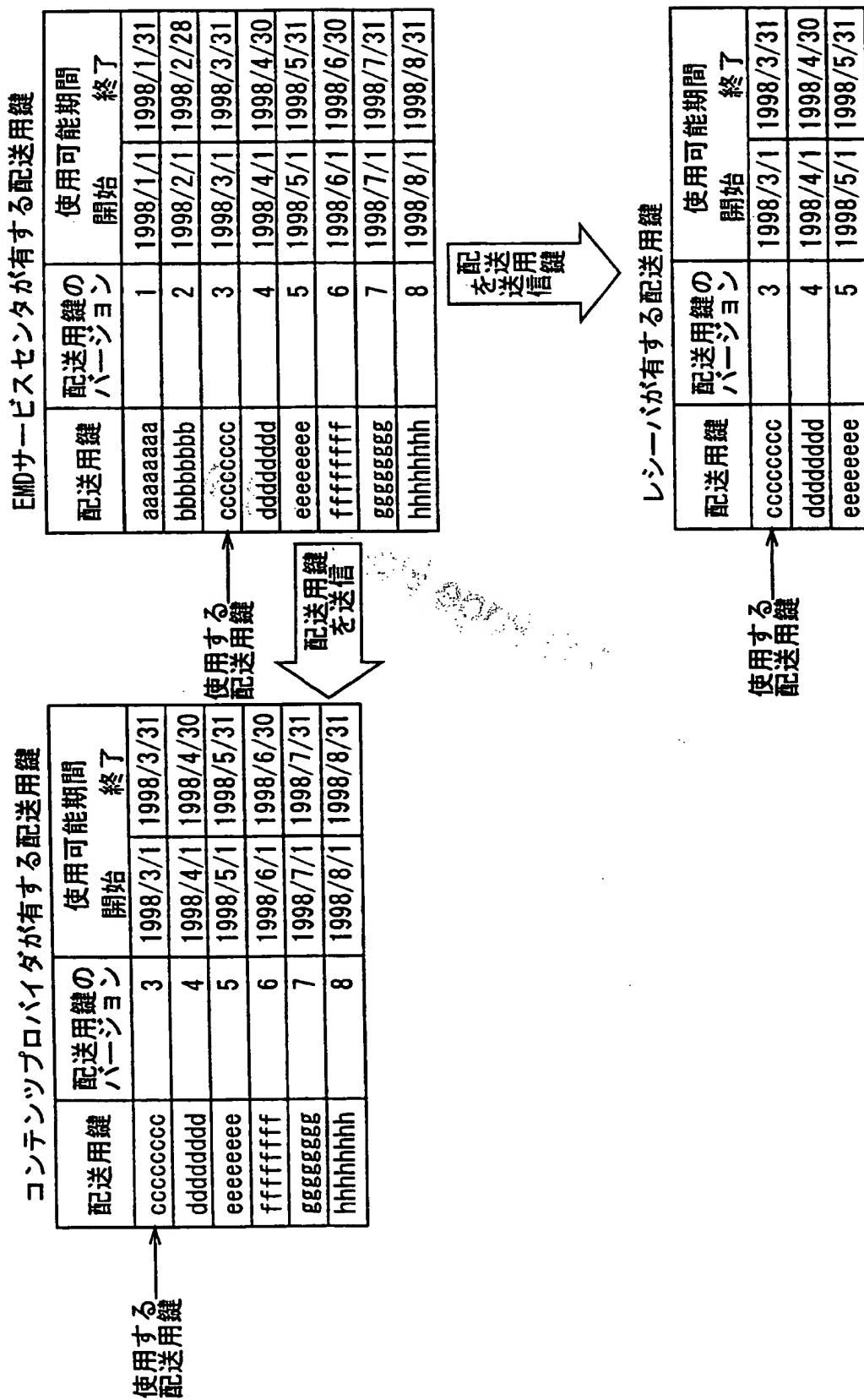


図 6

This Page Blank (uspto,

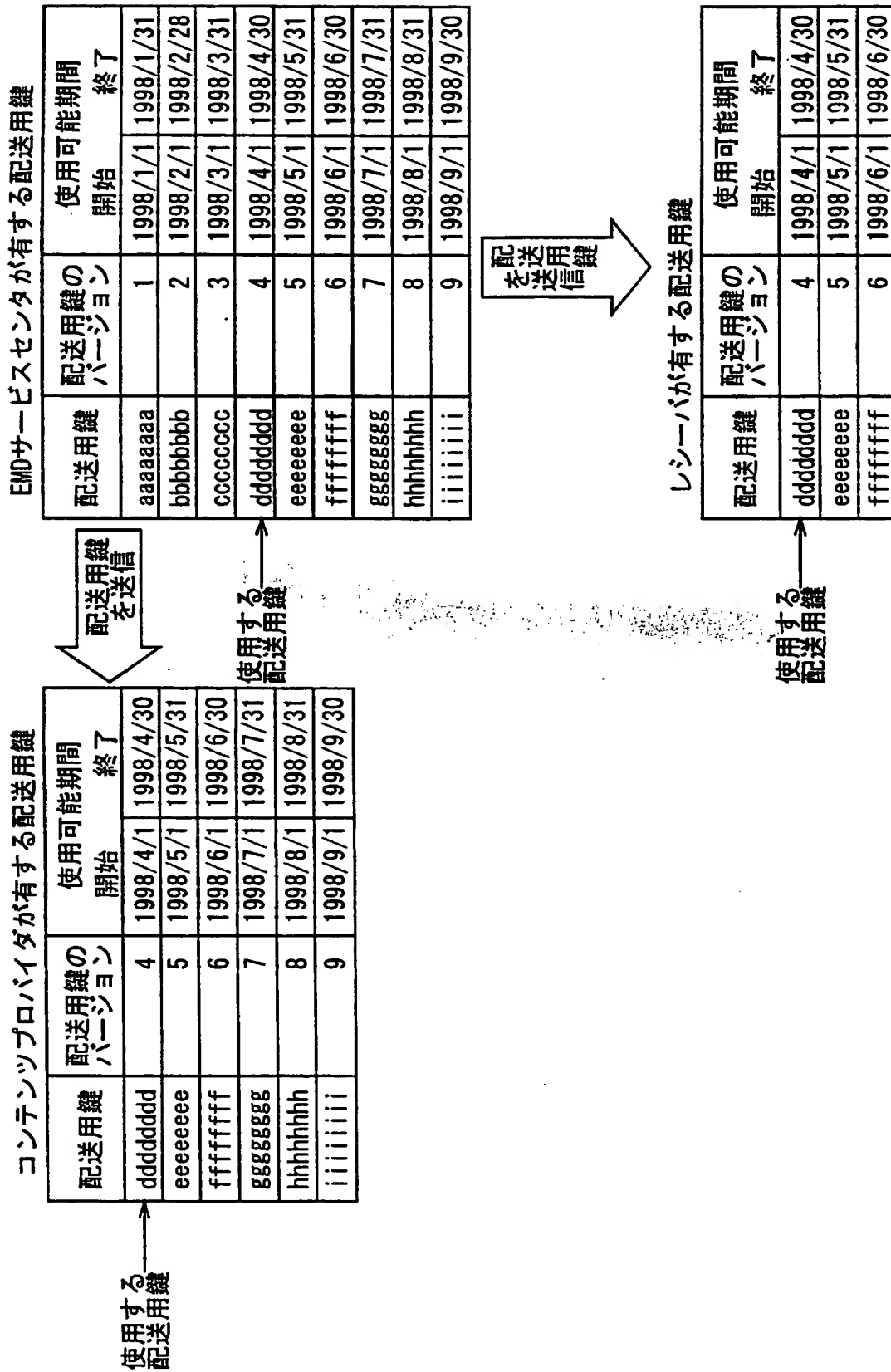


図 7

This Page Blank (uspto)

配送用鍵	配送用鍵の バージョン	使用可能期間	
		開始	終了
aaaaaaaa	1	1998/1/1	1998/1/31

仮配送用鍵Kd

図 8

This Page Blank (uspto)

SAMのID		SAM62のID	SAM212のID
機器番号		レシバ 51の機器番号 (100番)	レシバ 201の機器番号 (100番)
決済ID		ユーザFの決済ID	ユーザAの決済ID
決済 ユーザ 情報	氏名	ユーザFの氏名	ユーザAの氏名
	住所	ユーザFの住所	ユーザAの住所
	電話番号	ユーザFの電話番号	ユーザAの電話番号
	決済機関情報	ユーザFの決済情報	ユーザAの決済情報
	生年月日	ユーザFの生年月日	ユーザAの生年月日
	年齢	ユーザFの年齢	ユーザAの年齢(35才)
	性別	ユーザFの性別(男)	ユーザAの性別(男)
	ユーザのID	ユーザFのID	ユーザAのID
従属 ユーザ 情報	パスワード	ユーザFのパスワード	ユーザAのパスワード
	氏名		
	住所		
	電話番号		
	生年月日		
	性別		
	ユーザのID		
	パスワード		
利用ポイント情報		レシバ 51の利用 ポイント情報	レシバ 201の利用 ポイント情報

システム登録情報

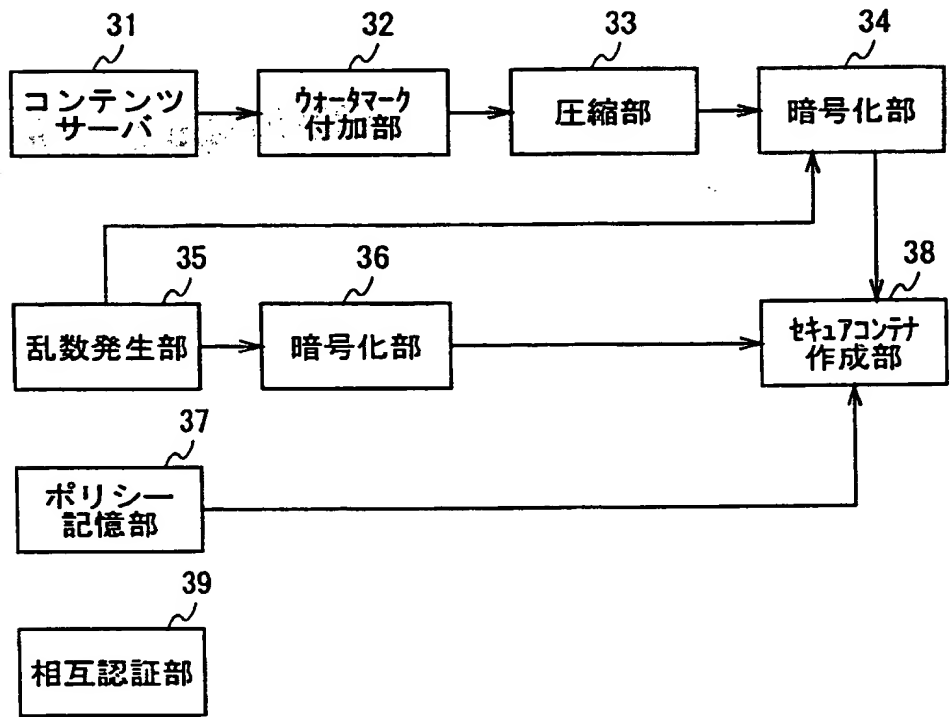
図 9

This Page Blank (uspto)

ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ2-1	222ポイント
	コンテンツプロバイダ2-2	123ポイント
	サービスプロバイダ3-1	345ポイント
	サービスプロバイダ3-2	0ポイント

利用ポイント情報

図 1 0



コンテンツプロバイダ 2-1

図 1 1

This Page Blank (uspto)

コンテンツのID	コンテンツAのID
コンテンツ「パ・イタ」のID	コンテンツ「パ・イタ」2-1のID
UCPのID	UCP8のID
UCPの有効期限	UCP8の有効期限
利用条件 20	ユーザ条件20 200ポイントより少ない
	機器条件20 条件なし
	ID 21 利用内容21のID
	形式21 Pay Per Play 4
	パ・イタ21 再生4回
	管理移動許可情報21 不可
利用内容 21	ID 22 利用内容22のID
	形式22 Pay Per Copy 2
	パ・イタ22 複製2回
	管理移動許可情報22 不可
利用内容 22	

UCPB

B

コンテンツのID	コンテンツAのID
コンテンツ「パ・イタ」のID	コンテンツ「パ・イタ」2-1のID
UCPのID	UCPAのID
UCPの有効期限	UCPAの有効期限
利用条件 10	ユーザ条件10 200ポイント以上
	機器条件10 条件なし
	ID 11 利用内容11のID
	形式11 買い取り再生
	パ・イタ11 ××××
	管理移動許可情報11 可
利用内容 11	ID 12 利用内容12のID
	形式12 第1世代複製
	パ・イタ12 ××××
	管理移動許可情報12 不可
利用内容 12	ID 13 利用内容13のID
	形式13 期間制限再生
	パ・イタ13 ××××
	管理移動許可情報13 不可
利用内容 13	ID 14 利用内容14のID
	形式14 Pay Per Copy 5
	パ・イタ14 複製5回
	管理移動許可情報14 不可
利用内容 14	

UCPA

図 1 2

This Page Blank (uspto)

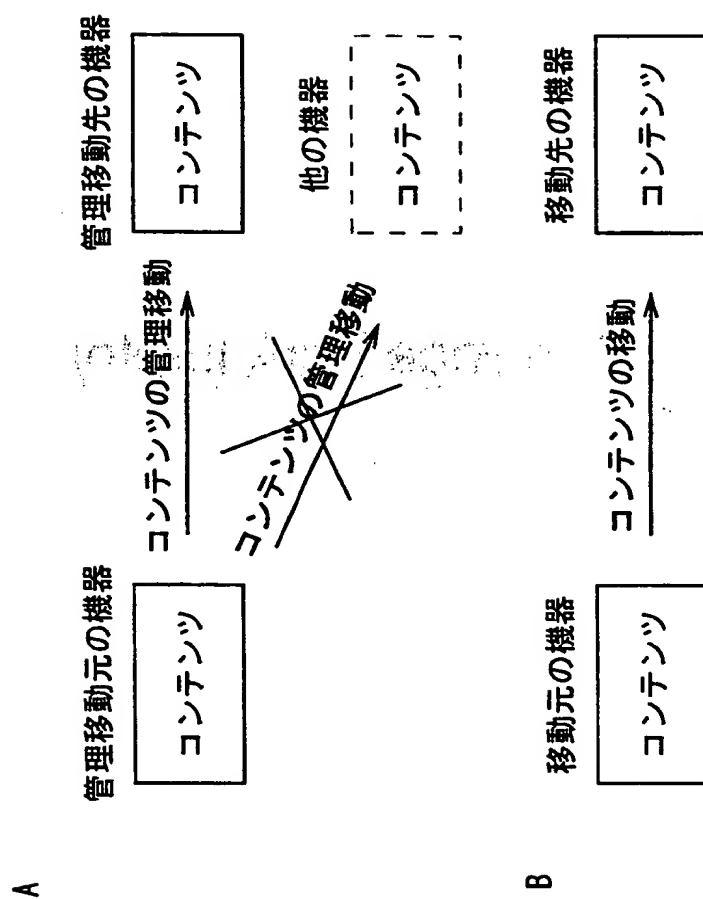


図 13

Page Blank (uspto)

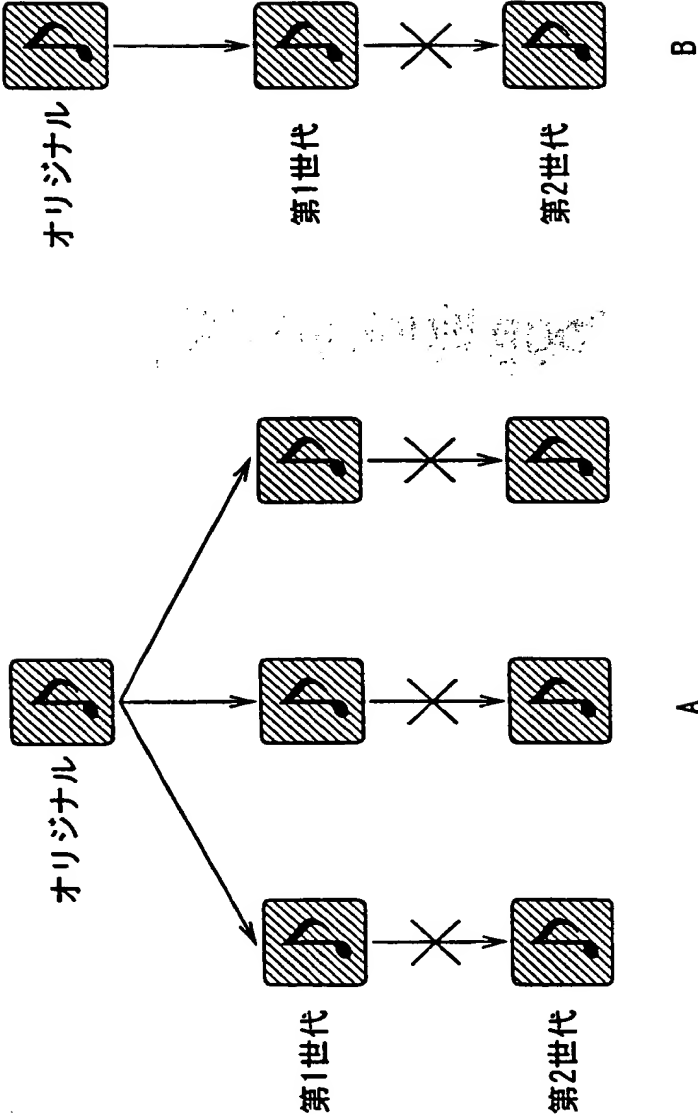


図 1 4

This Page Blank (uspto)

A

サービスコード	意味
0000h	条件なし
0001h乃至00FFh	機器に関し条件有り
0100h乃至01FFh	性別条件あり
0200h乃至02FFh	年齢条件あり
0300h乃至7FFFh	その他の条件あり
8000h乃至FFFFh	利用ポイントに関し条件有り

B

コンディションコード	意味
00h	無条件
01h	=
02h	≠
03h	<(より小さい)
04h	>(より大きい)
05h	≤(以下)
06h	≥(以上)
07h乃至FFh	空き

図 1 5

This Page Blank (uspto)

A

ユーザ条件 10	サービスコード	ハッシュコード	コンディションコード
	80 × × h	0000C8h	06h
機器条件 10	サービスコード	ハッシュコード	コンディションコード
	0000h	FFFFFFh	00h

UCPAの利用条件 10

B

ユーザ条件 20	サービスコード	ハッシュコード	コンディションコード
	80 × × h	0000C8h	03h
機器条件 20	サービスコード	ハッシュコード	コンディションコード
	0000h	FFFFFFh	00h

UCPBの利用条件 20

図 16

This Page Blank (uspto)

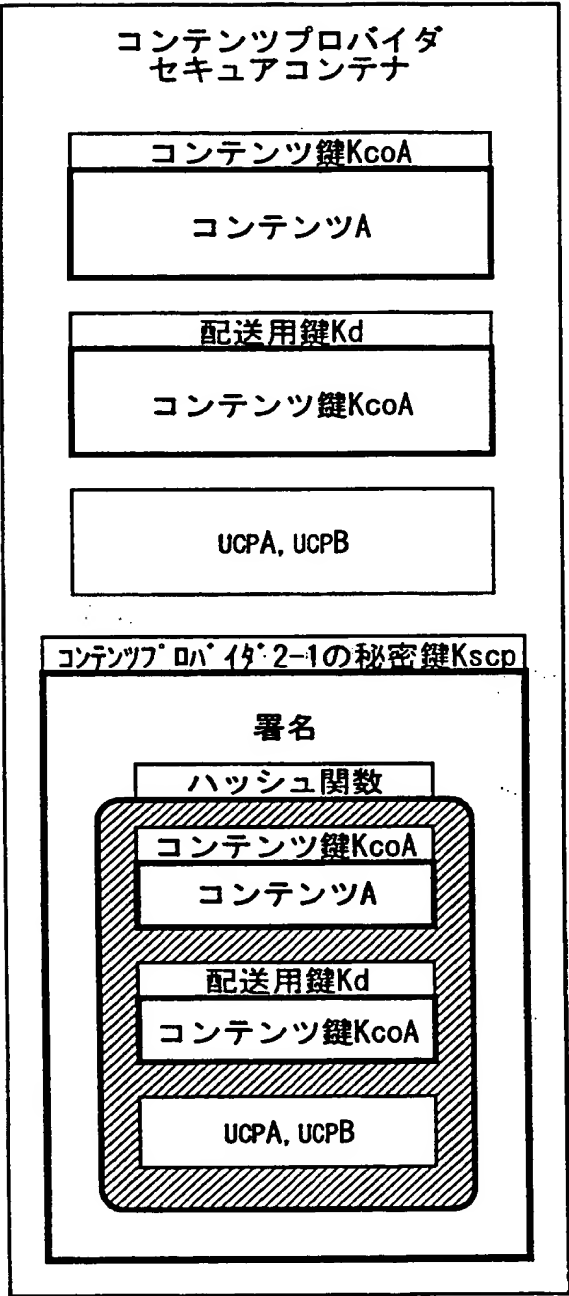


図 1 7

This Page Blank (uspto)

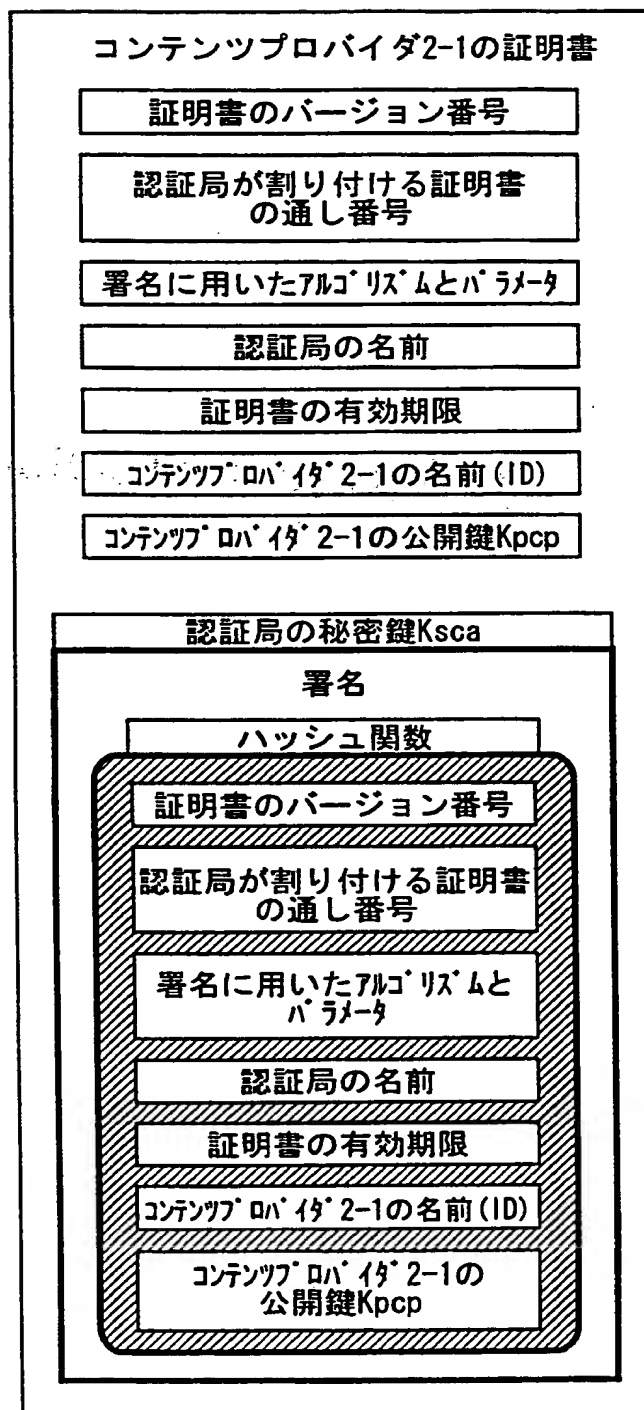
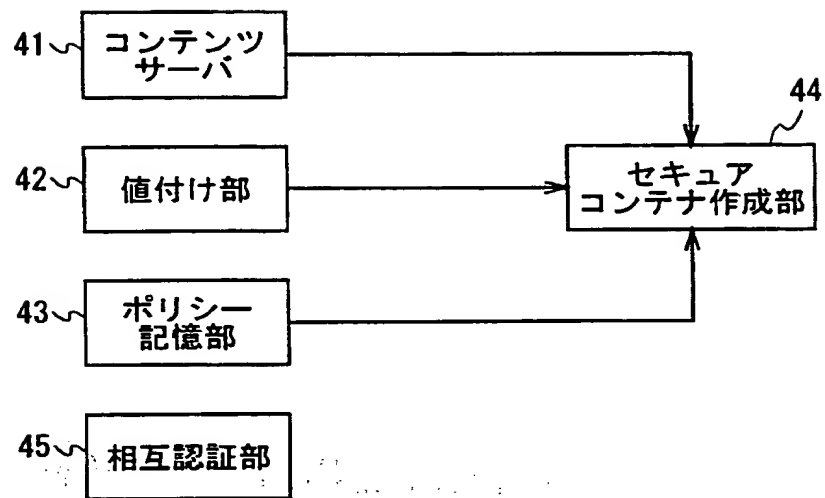


図 18

This Page Blank (uspto)



サービスプロバイダ 3-1

図 19

This Page Blank (uspto)

A	コンテンツのID	コンテンツAのID
	コンテンツAのID	コンテンツAのID 2-1のID
	UCPのID	UCPのID
	サブスクリプションのID	サブスクリプション 3-1のID
	PTのID	PTA-1のID
	PTの有効期限	PTA-1の有効期限
	価格条件 10	ユーザ条件 10
		機器条件 10
	価格内容 11	2000円
	価格内容 12	600円
B	価格内容 13	100円
	価格内容 14	300円
	コンテンツのID	コンテンツAのID
	コンテンツAのID	コンテンツAのID 2-1のID
	UCPのID	UCPのID
	サブスクリプションのID	サブスクリプション 3-1のID
	PTのID	PTA-2のID
	PTの有効期限	PTA-2の有効期限
	価格条件 20	ユーザ条件 20
		機器条件 20
PTA-1	価格内容 21	1000円
	価格内容 22	300円
	価格内容 23	50円
	価格内容 24	150円
	コンテンツのID	コンテンツAのID
	コンテンツAのID	コンテンツAのID 2-1のID
	UCPのID	UCPのID
	サブスクリプションのID	サブスクリプション 3-1のID
	PTのID	PTA-2のID
	PTの有効期限	PTA-2の有効期限
PTA-2	価格条件 20	ユーザ条件 20
		機器条件 20
	価格内容 21	1000円
	価格内容 22	300円
	価格内容 23	50円
	価格内容 24	150円
	コンテンツのID	コンテンツAのID
	コンテンツAのID	コンテンツAのID 2-1のID
	UCPのID	UCPのID
	サブスクリプションのID	サブスクリプション 3-1のID

図 20

This Page Blank (uspto)

A

ユーザ条件 10	サービスコード	ハッシュコード	コンディションコード
	01 × × h	000000h	01h
機器条件 10	サービスコード	ハッシュコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-1の価格条件 10

B

ユーザ条件 20	サービスコード	ハッシュコード	コンディションコード
	01 × × h	000001h	01h
機器条件 20	サービスコード	ハッシュコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-2の価格条件 20

図 2 1

This Page Blank (uspto)

コンテンツのID	コンテンツAのID
コンテンツAのID	コンテンツAのID 2-1のID
UCPのID	UCPのID
サブスクリプションのID	サブスクリプション 3-1のID
PTのID	PTB-2のID
PTの有効期限	PTB-2の有効期限
価格条件 40	ユーザ条件 40
	機器条件 40
価格内容 41	50円
価格内容 42	150円

PTB-2
B

コンテンツのID	コンテンツAのID
コンテンツAのID	コンテンツAのID 2-1のID
UCPのID	UCPのID
サブスクリプションのID	サブスクリプション 3-1のID
PTのID	PTB-1のID
PTの有効期限	PTB-1の有効期限
価格条件 30	ユーザ条件 30
	機器条件 30
価格内容 31	100円
価格内容 32	300円

PTB-1
A

図 2 2

This Page Blank (uspto)

A

ユーザ条件 30	サービスコード	ハッシュコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 30	サービスコード	ハッシュコード	コンディションコード
	00××h	000064h	03h

PTB-1の価格条件 30

B

ユーザ条件 40	サービスコード	ハッシュコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 40	サービスコード	ハッシュコード	コンディションコード
	00××h	000064h	06h

PTB-2の価格条件 40

図 2 3

This Page Blank (uspto)

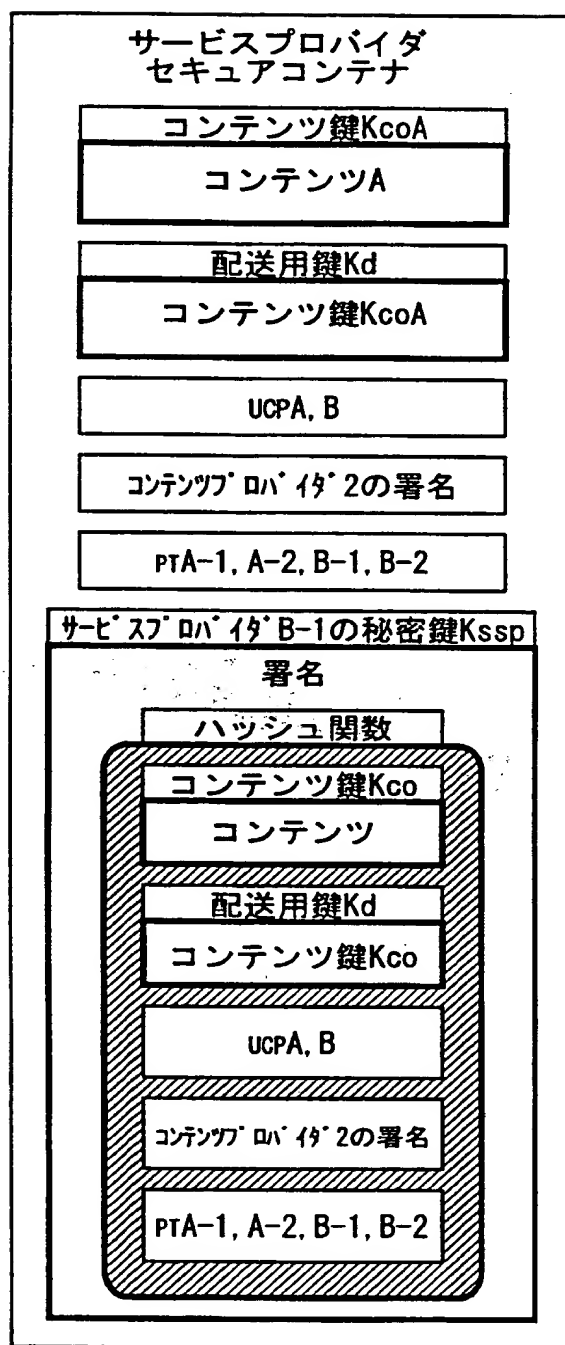


図 2 4

This Page Blank (uspto)

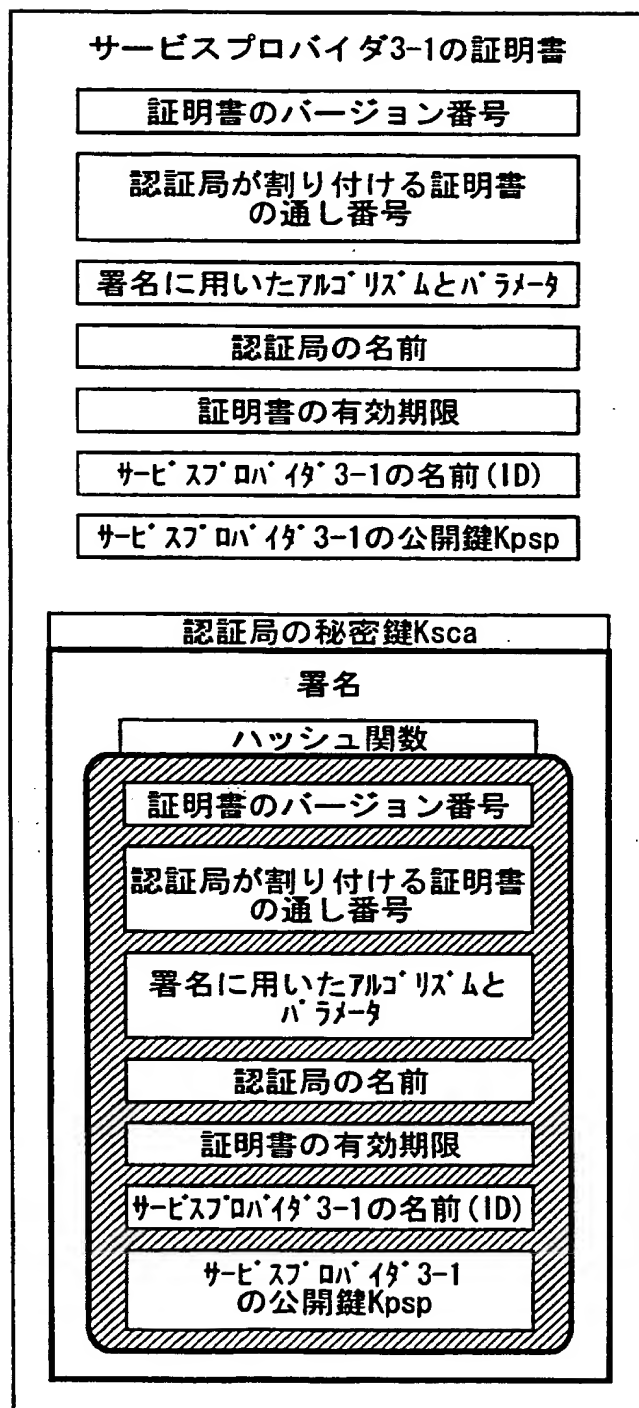


図 2 5

This Page Blank (uspto)

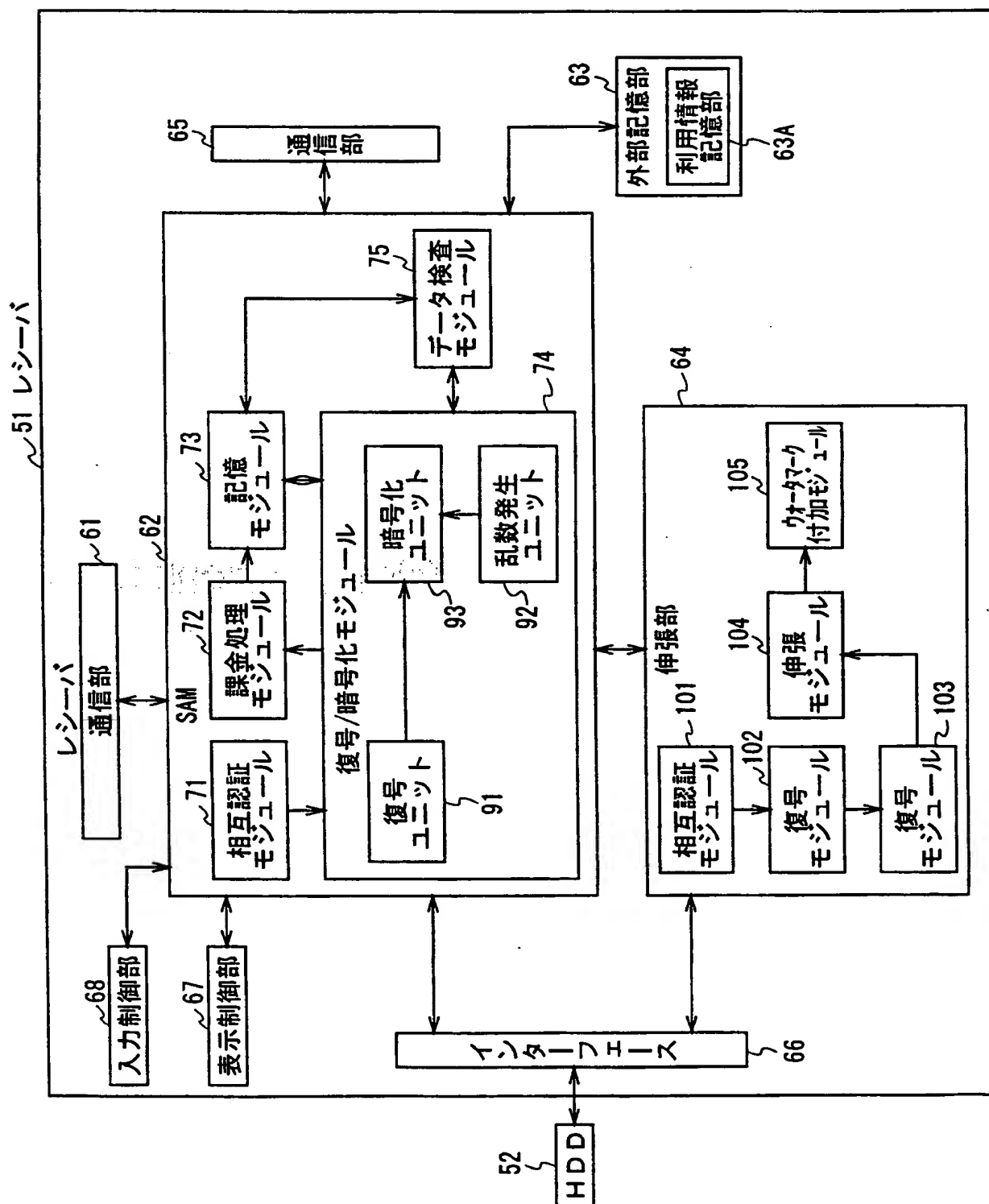


図 26

This Page Blank (uspto)

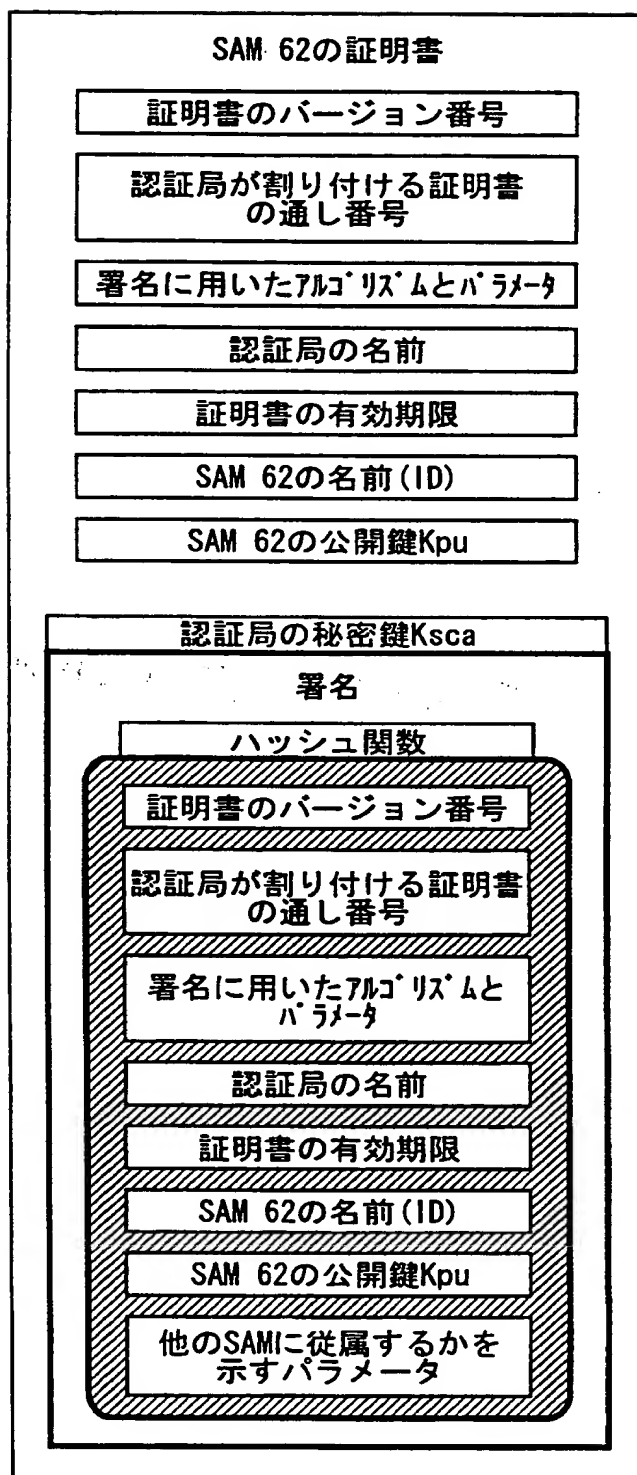


図 2 7

This Page Blank (uspto)

コンテンツのID	コンテンツAのID
コンテンツのID	コンテンツ 2-1のID
UCPのID	ucpAのID
UCPの有効期限	ucpAの有効期限
サービスのID	サービス 3-1のID
PTのID	ptA-1のID
PTの有効期限	ptA-1の有効期限
UCSのID	ucsAのID
SAMのID	SAM62のID
ユーザのID	ユーザFのID
利用内容	ID
	形式
	パラメータ
	管理移動状態情報
利用履歴	

ucsA

図 2 8

This Page Blank (uspto)

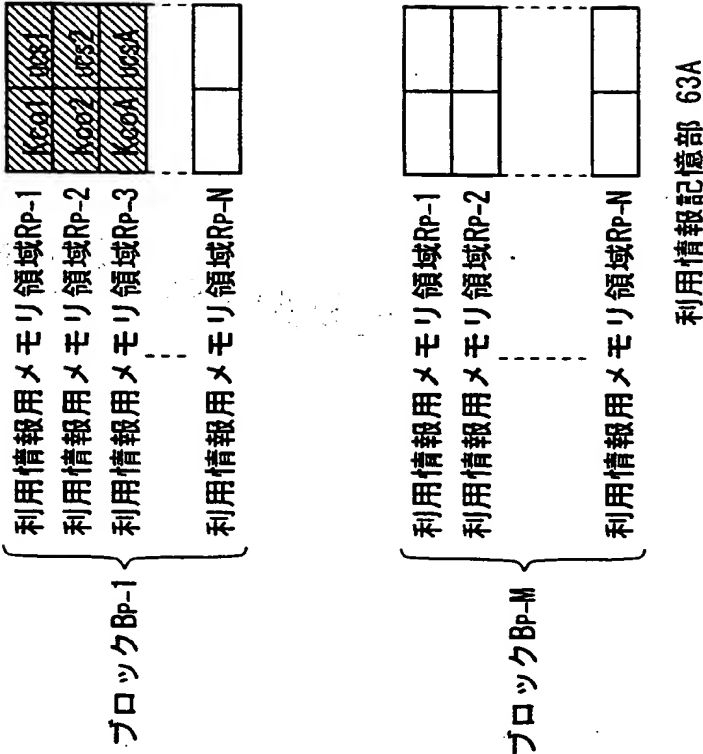


図 2 9

This Page Blank (uspto)

コンテンツのID		コンテンツAのID
コンテンツパライタのID		コンテンツパライタ2-1のID
UCPのID		ucPAのID
UCPの有効期限		ucPAの有効期限
サービスパライタのID		サービスパライタ3-1のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		ucsAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容11のID
	形式	買い取り再生
	パラメータ	× × ×
	管理移動状態情報	管理移動元: SAM62のID、 管理移動先: SAM62のID
課金履歴		× × ×

課金情報 A

図 3 0

This Page Blank (uspto)

SAM62の公開鍵Kpu		
SAM62の秘密鍵Ksu		
EMDサービスセンタ1の公開鍵Kpesc		
認証局の公開鍵Kpca		
保存用鍵Ksave		
3月分の配送用鍵Kd		
⋮		
SAM62証明書		
基準情報 51		
課金情報		
⋮		
検査値Hp-1	検査値Hp-2
.....	検査値Hp-M	

図 3 1

This Page Blank (uspto)

SAMのID		SAM62のID	
機器番号		レシーバ 51の機器番号 (100番)	
決済ID		ユーザFの決済ID	
課金の上限額		正式登録時の 課金の上限額	
決済ユーザ情報	氏名	ユーザFの氏名	
	住所	ユーザFの住所	
	電話番号	ユーザFの電話番号	
	決済機関情報	ユーザFの決済機関情報	
	生年月日	ユーザFの生年月日	
	年齢	ユーザFの年齢(21才)	
	性別	ユーザFの性別(男)	
	ユーザのID	ユーザFのID	
	パスワード	ユーザFのパスワード	
従属ユーザ情報	氏名		
	住所		
	電話番号		
	生年月日		
	性別		
	ユーザのID		
	パスワード		
利用ポイント情報		レシーバ 51の利用 ポイント情報	

基準情報 51

図 3 2

This Page Blank (uspto)

ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ 2-1	222ポイント
	コンテンツプロバイダ 2-2	123ポイント
	サービスプロバイダ 3-1	345ポイント
	サービスプロバイダ 3-2	0ポイント

基準情報51の利用ポイント情報

図 3 3

This Page Blank (uspto)

ユーザ51の登録条件

ユーザ201の登録リスト

リスト部

SAM ID	ユーザID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態フラグ	登録条件署名	登録リスト署名
SAM62のID	ユーザFのID	可	可	SAM62のID	なし	制限なし	××××	××××
SAM212のID	ユーザAのID	可	可	SAM212のID	なし	制限なし	××××	

対象SAM ID

SAM62のID

有効期限

××××

ページ番号

××××

接続されている機器数

2

対象SAM情報部

図 3 4

This Page Blank (uspto)

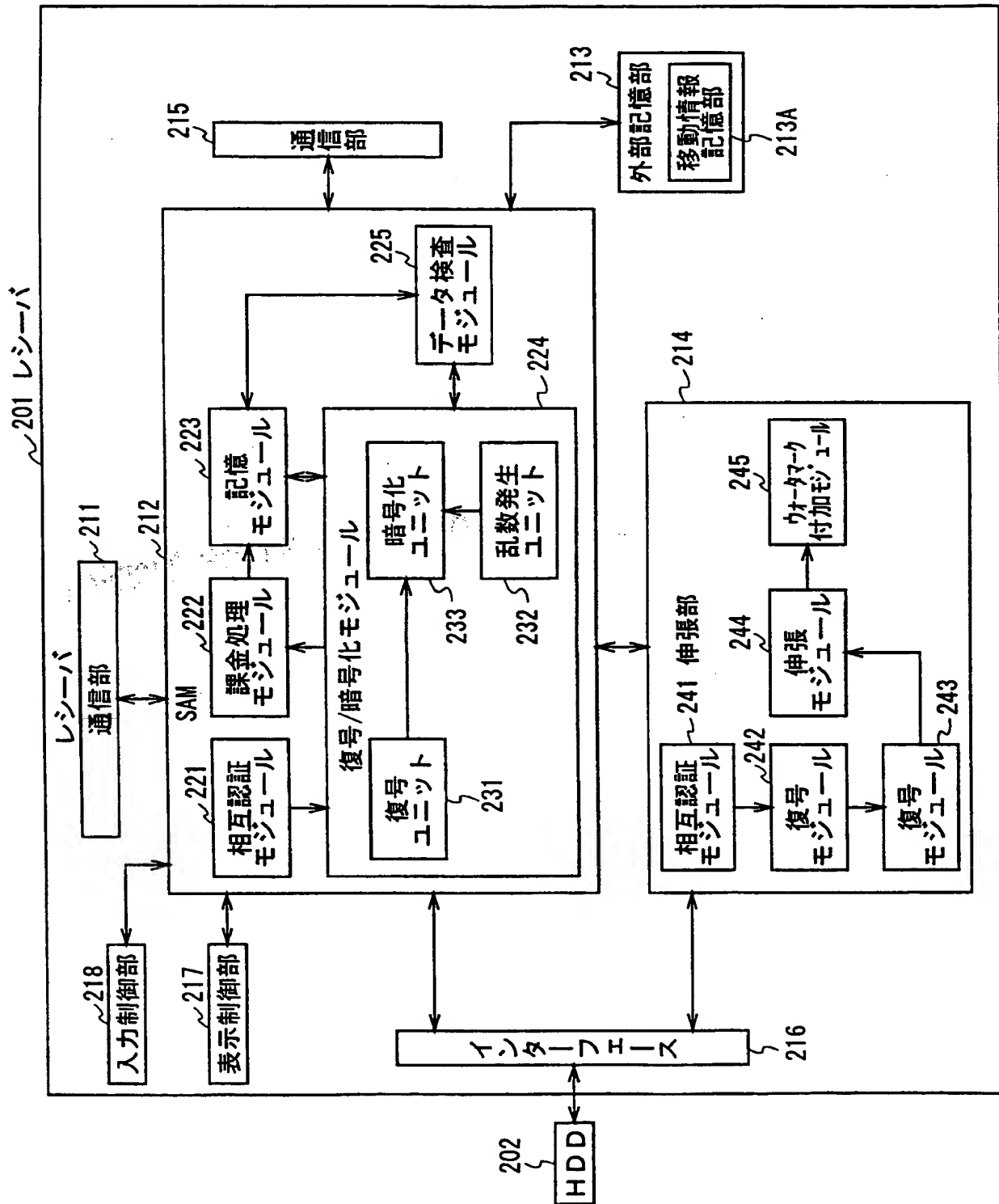


図 35

This Page Blank (uspto)

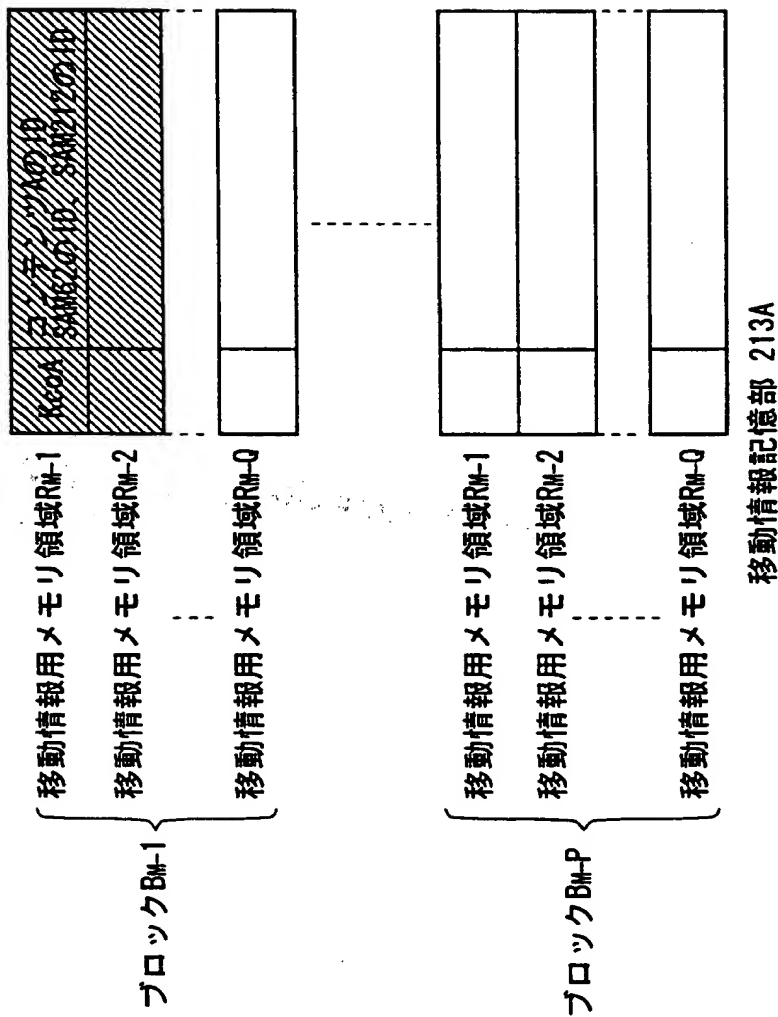


図 3 6

This Page Blank (uspto)

SAM212の公開鍵Kpu		
SAM212の公開鍵Ksu		
EMDサービスセンタ1の公開鍵Kpesc		
認証局の公開鍵Kpca		
保存用鍵Ksave		
3月分の配送用鍵Kd		
⋮		
SAM212証明書		
基準情報 201		
⋮		
検査値Hm-1	検査値Hm-2
.....		検査値Hm-P

図 3 7

This Page Blank (uspto)

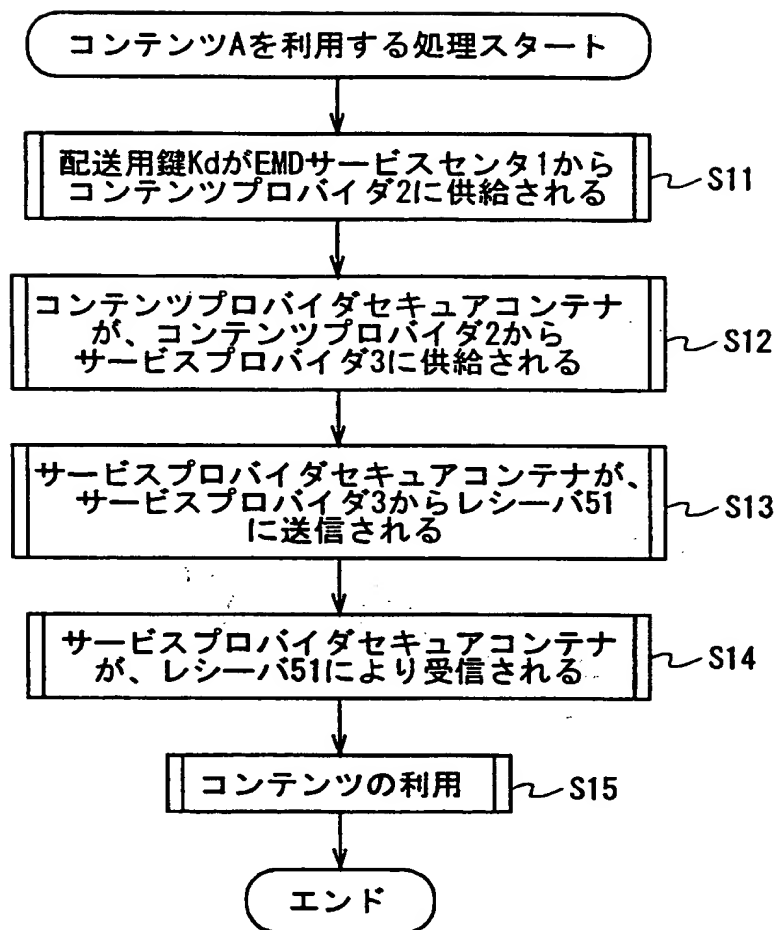


図 3 8

This Page Blank (uspto)

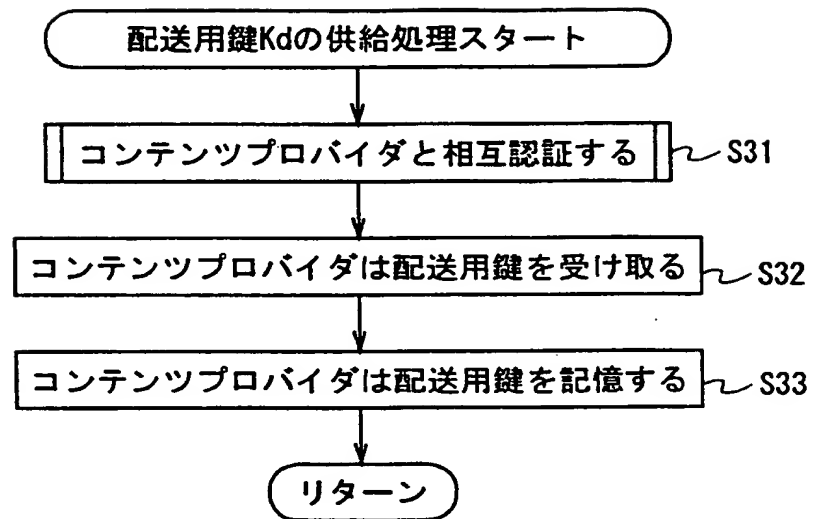


図 39

This Page Blank (uspto)

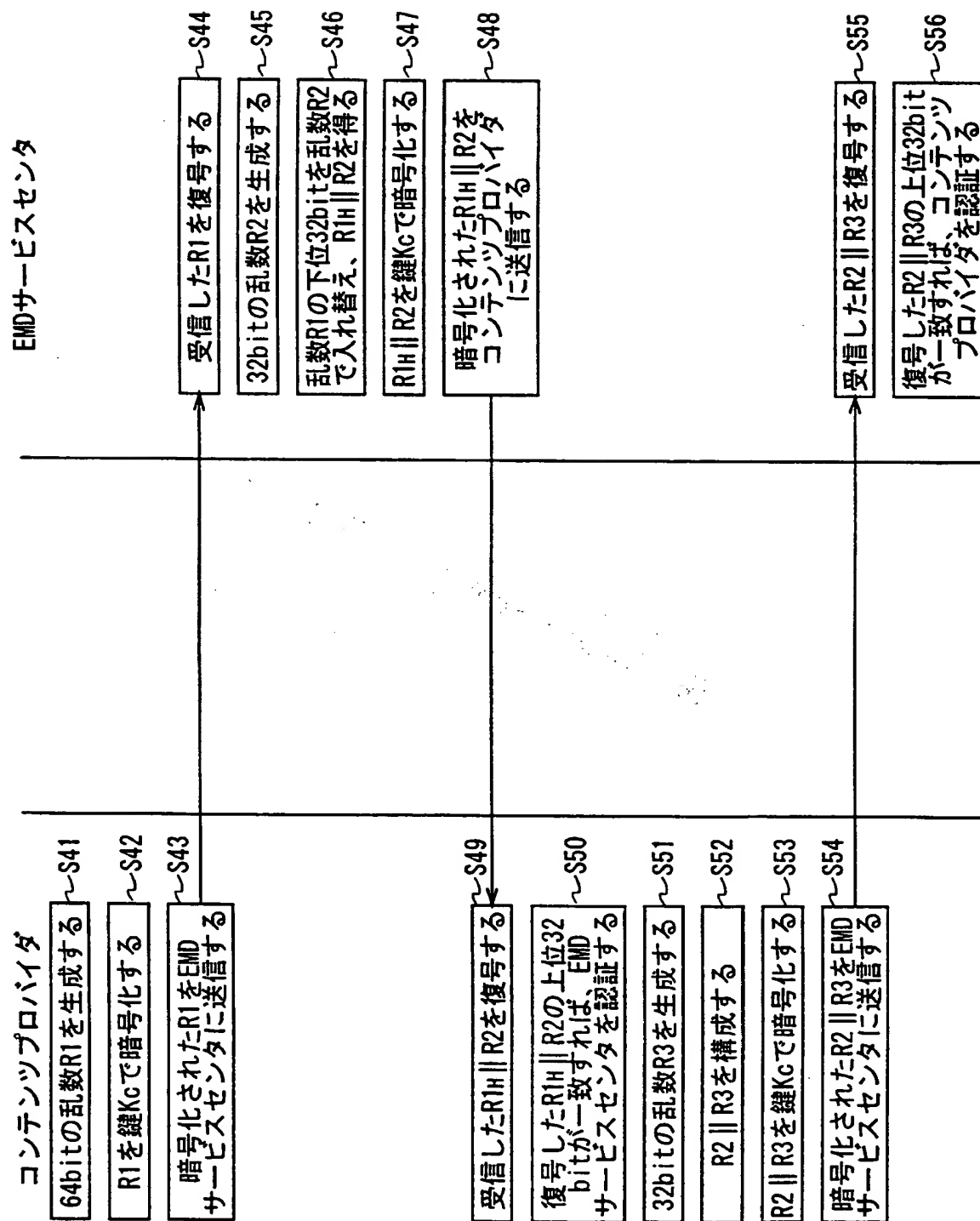


図 40

This Page Blank (uspto)

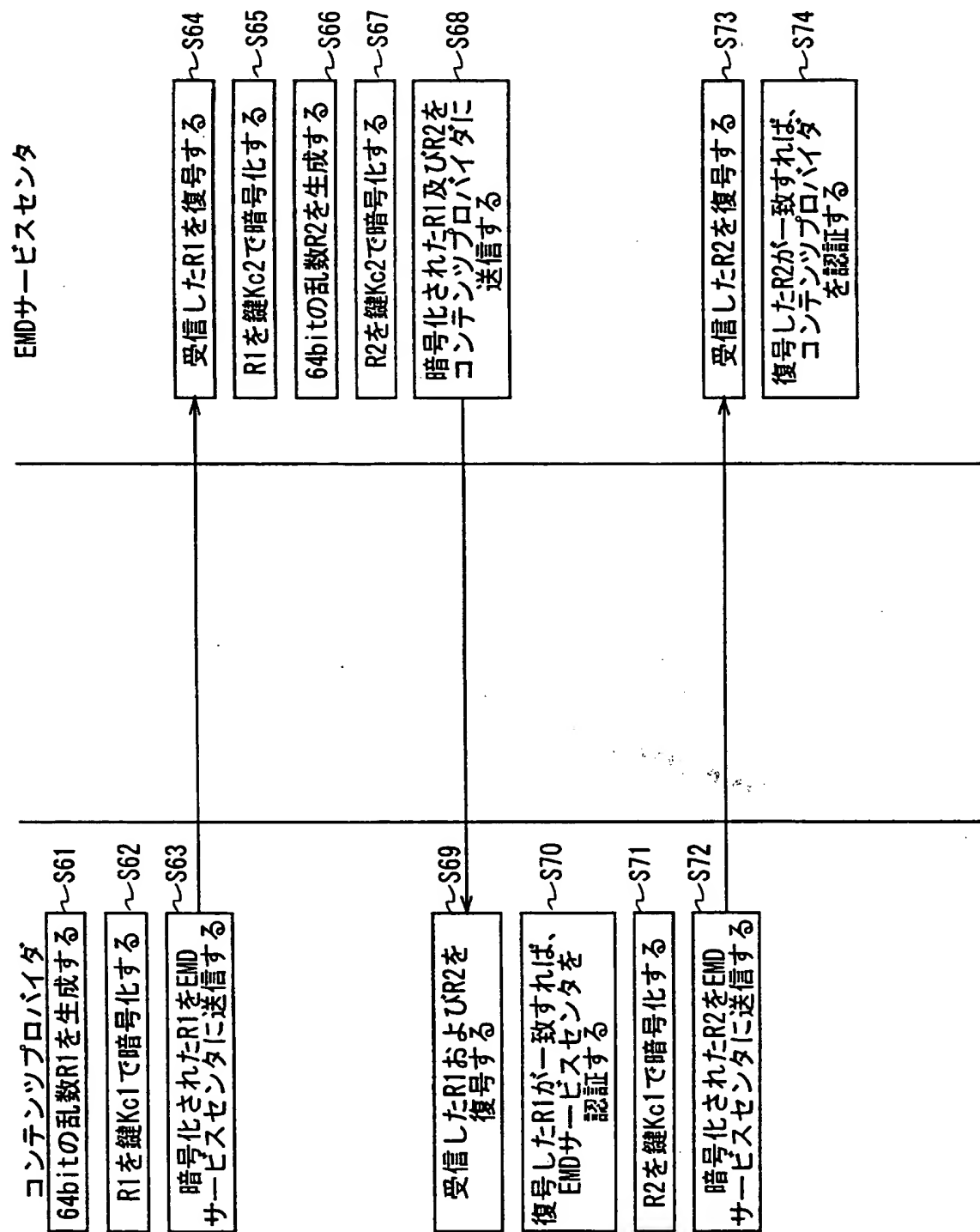


図 4 1

This Page Blank (uspto)

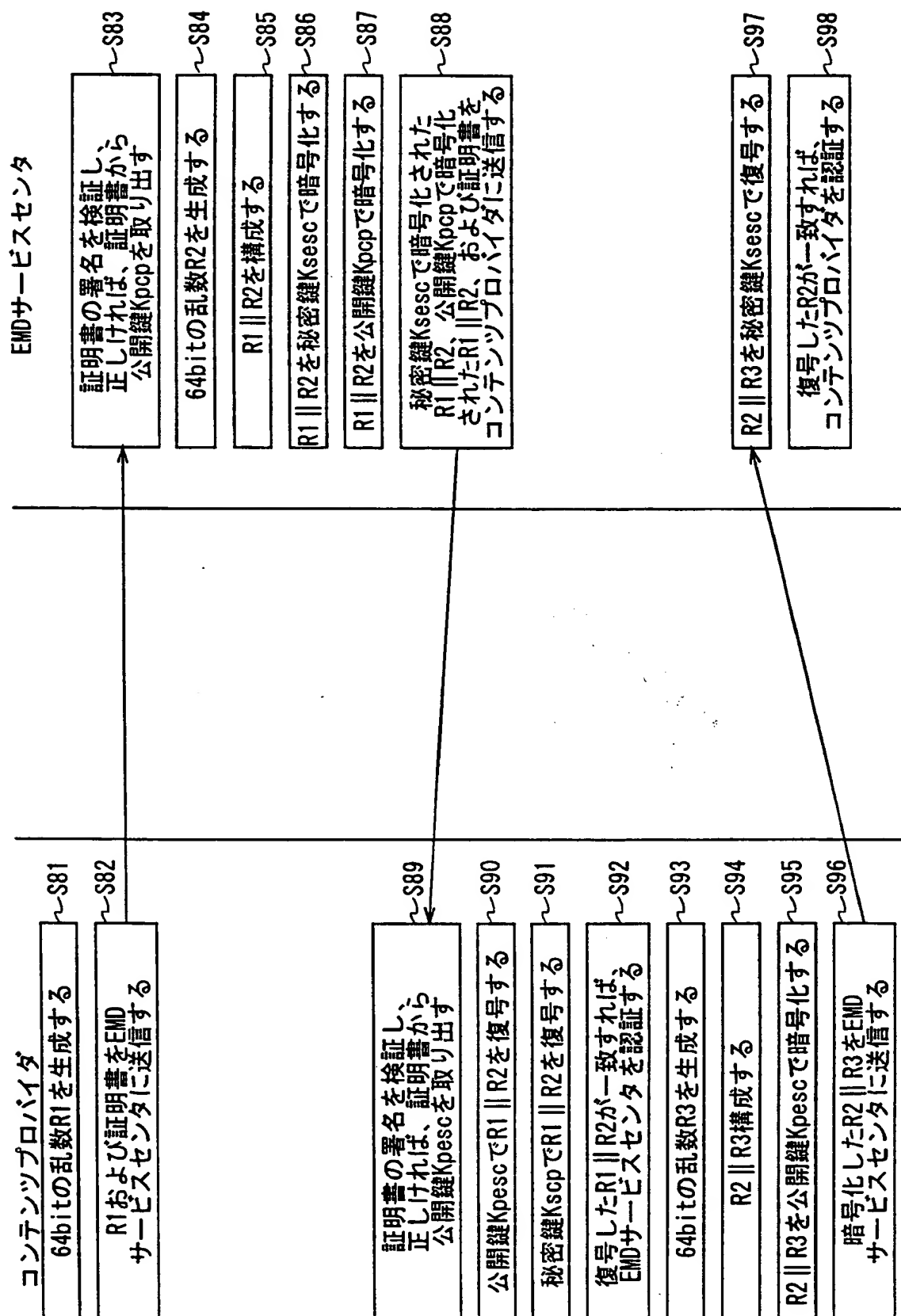


図 4 2

This Page Blank (uspto)

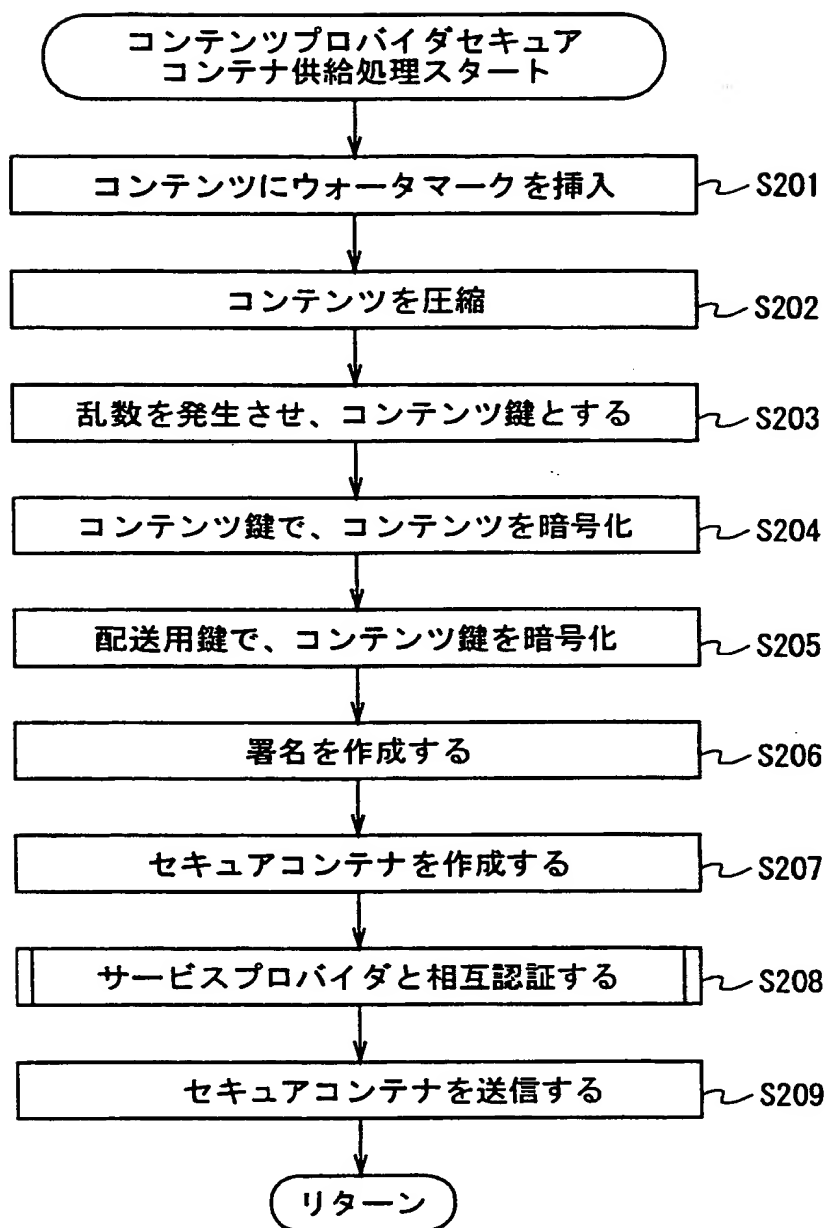


図 4 3

This Page Blank (uspto)

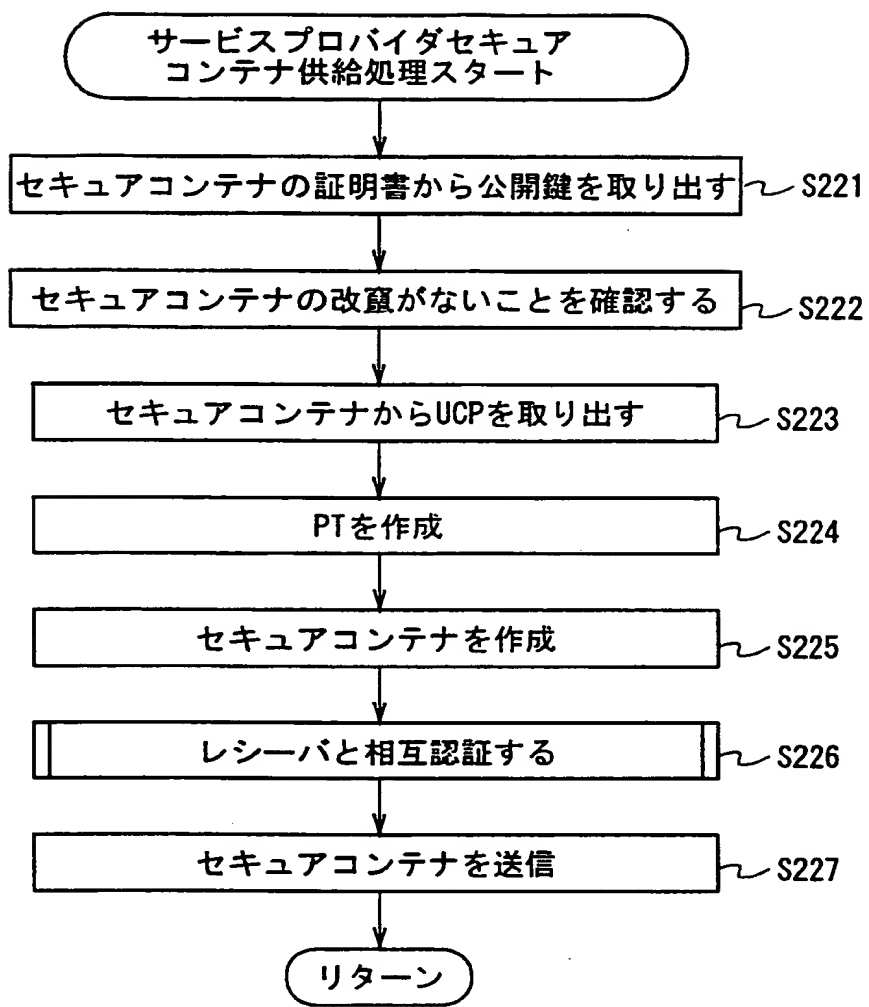


図 4 4

THIS Page Blank (uspto)

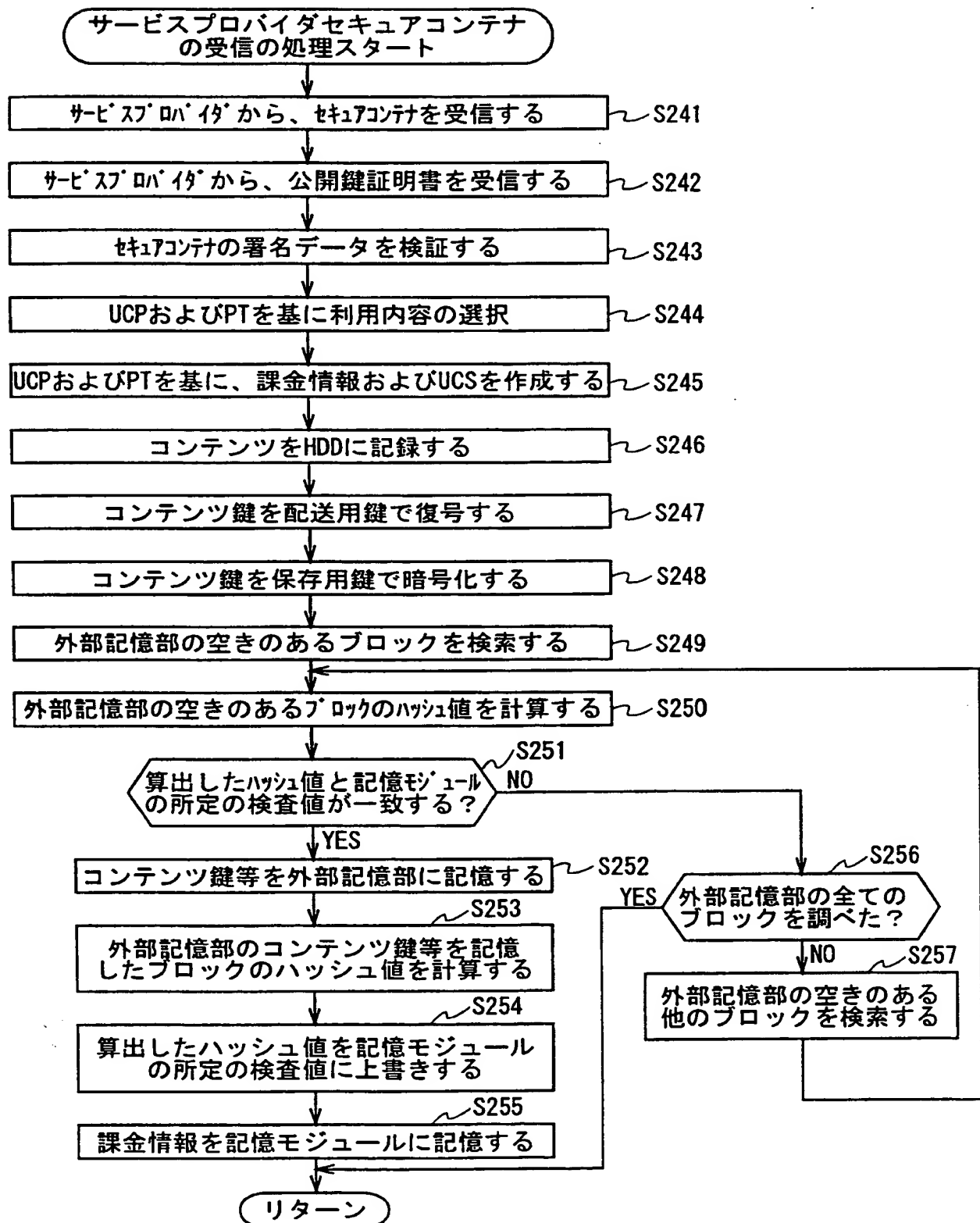


図 4 5

This Page Blank (uspto)

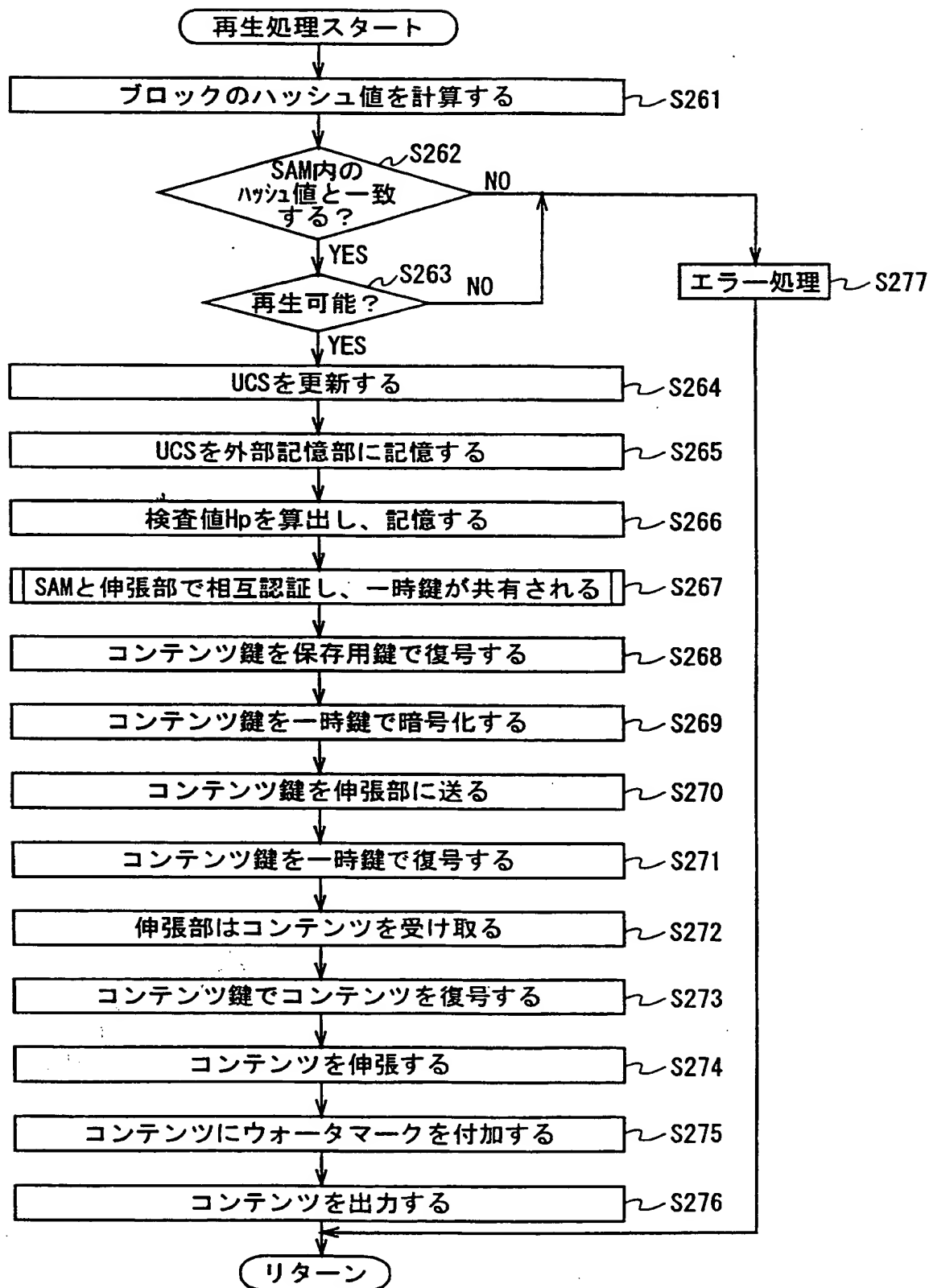


図 4 6

This Page Blank (uspto)

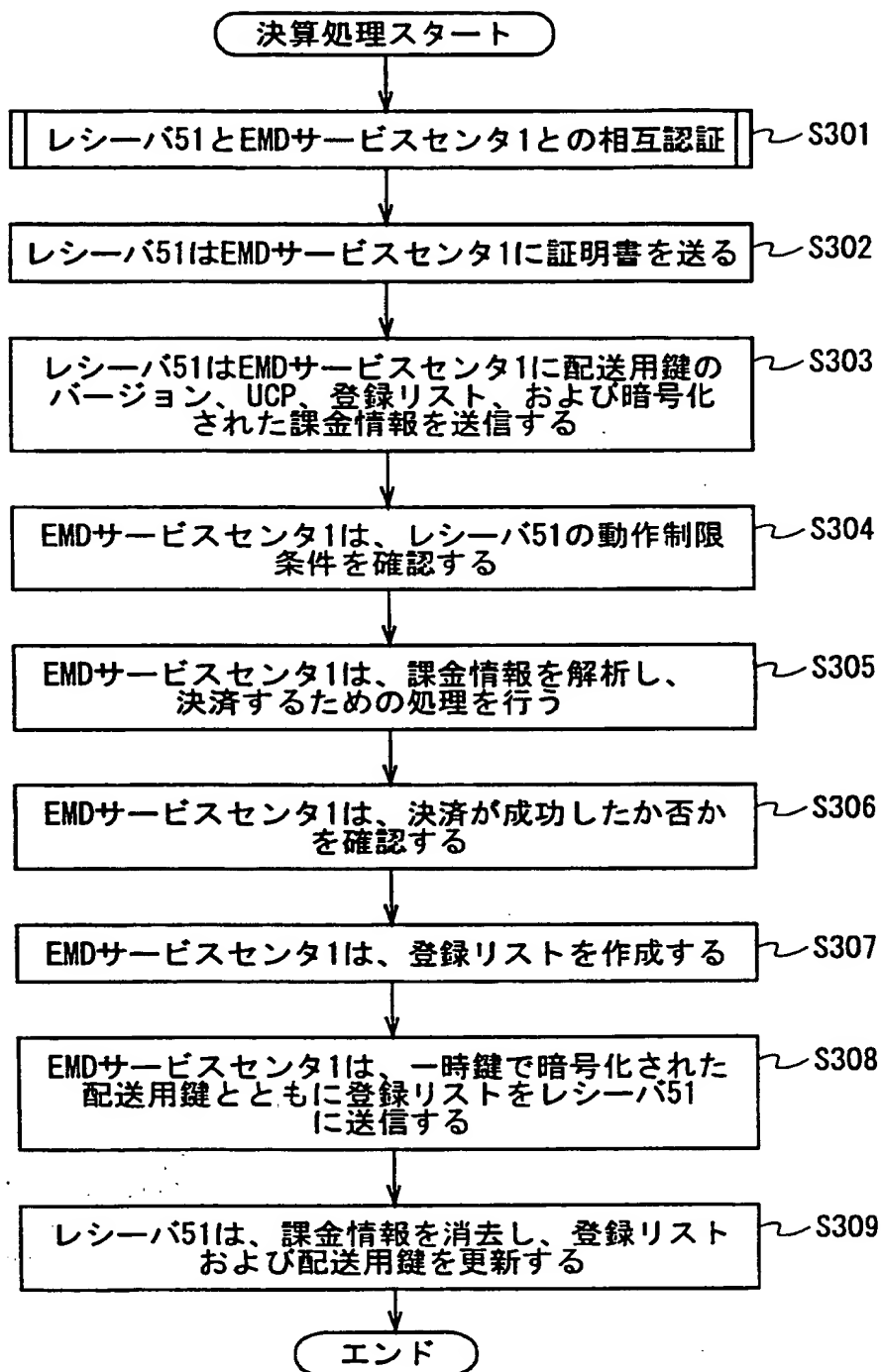


図 4 7

This Page Blank (uspto)

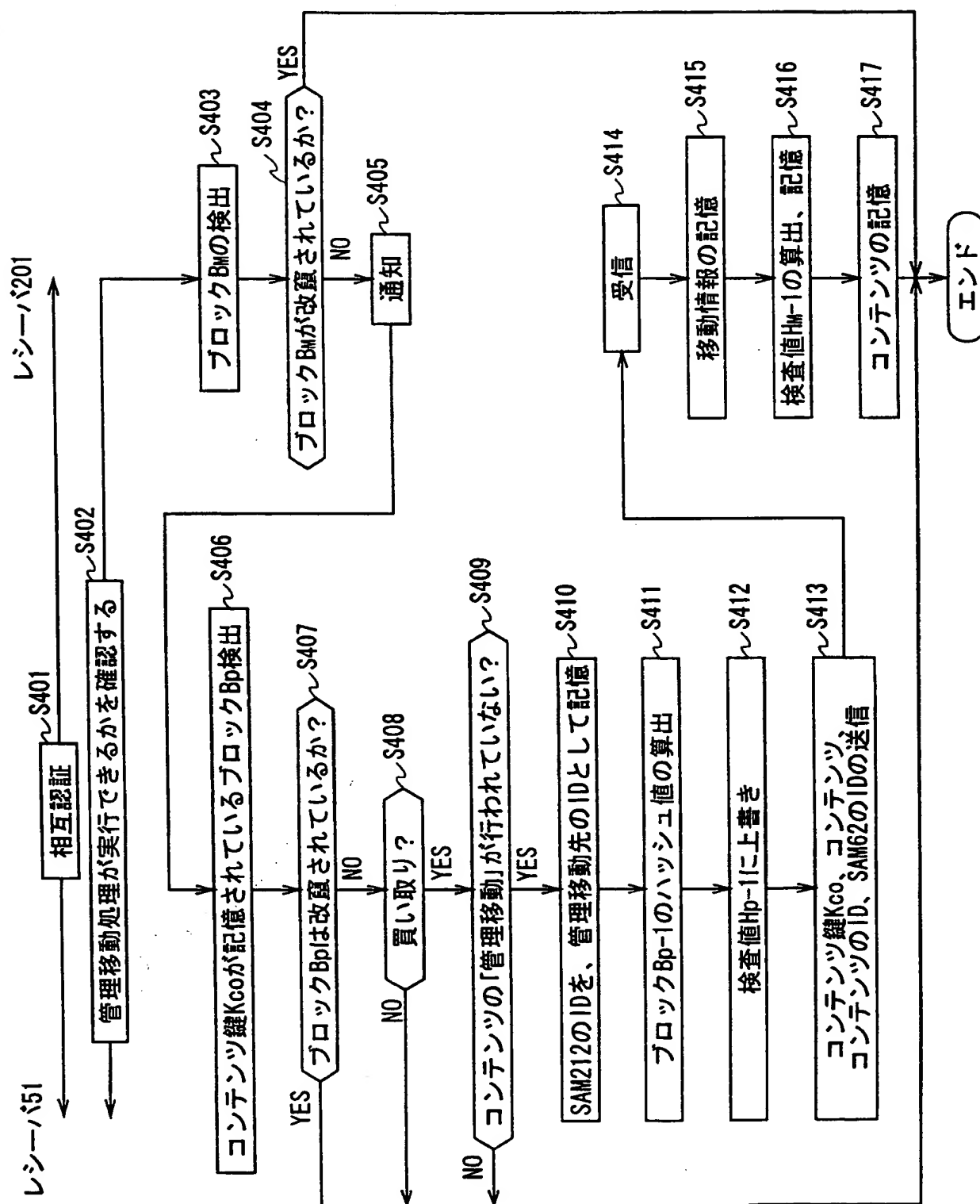
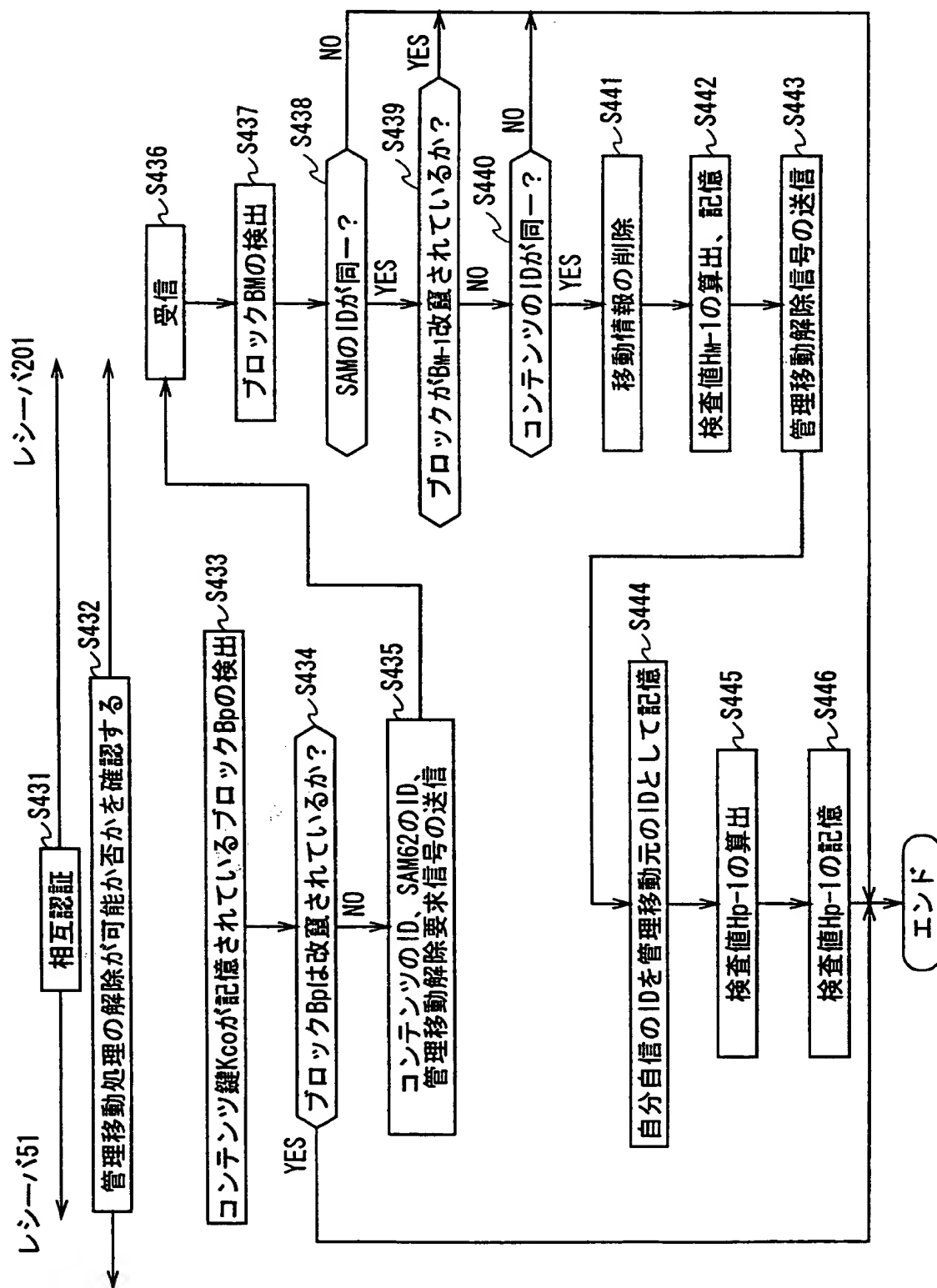


図 48

This Page Blank (uspto)



94 図

This Page Blank (uspto)

符 号 の 説 明

1 . . . EMDサービスセンタ, 2 . . . コンテンツプロバイダ, 3 . . . サービスプロバイダ, 5 . . . ユーザホームネットワーク, 11 . . . サービスプロバイダ管理部, 12 . . . コンテンツプロバイダ管理部, 13 . . . 著作権管理部, 14 . . . 鍵サーバ, 15 . . . 経歴データ管理部, 16 . . . 利益分配部, 17 . . . 相互認証部, 18 . . . ユーザ管理部, 19 . . . 課金請求部, 20 . . . 出納部, 21 . . . 監査部, 31 . . . コンテンツサーバ, 32 . . . ウォータマーク付加部, 33 . . . 圧縮部, 34 . . . 暗号化部, 35 . . . 乱数発生部, 36 . . . 暗号化部, 37 . . . ポリシー記憶部, 38 . . . セキュアコンテナ作成部, 39 . . . 相互認証部, 41 . . . コンテンツサーバ, 42 . . . 値付け部, 43 . . . ポリシー記憶部, 44 . . . セキュアコンテナ作成部, 45 . . . 相互認証部, 51 . . . レシーバ, 52 . . . HDD, 61 . . . 通信部, 62 . . . SAM, 63 . . . 外部記憶部, 64 . . . 伸張部, 65 . . . 通信部, 66 . . . インタフェース, 67 . . . 表示制御部, 68 . . . 入力制御部, 71 . . . 相互認証モジュール, 72 . . . 課金処理モジュール, 73 . . . 記憶モジュール, 74 . . . 復号/暗号化モジュール, 75 . . . データ検査モジュール, 91 . . . 復号ユニット, 92 . . . 乱数発生ユニット, 93 . . . 暗号化ユニット, 101 . . . 相互認証モジュール, 102 . . . 復号モジュール, 103 . . . 復号モジュール, 104 . . . 伸張モジュール, 105 . . . ウォータマーク付加モジュール, 201 . . . レシーバ, 202 . . . HDD, 211 . . . 通信部, 212 . . . SAM, 213 . . . 外部記憶部, 214 . . . 伸張部, 215 . . . 通信部, 216 . . . インタフェース, 217 . . . 表示制御部, 218 . . . 入力制御部, 221 . . . 相

This Page Blank (uspto)

互認証モジュール, 2 2 2 . . . 課金処理モジュール, 2 2 3 . . . 記憶モジュール, 2 2 4 . . . 復号/暗号化モジュール, 2 2 5 . . . データ検査モジュール, 2 3 1 . . . 復号ユニット, 2 3 2 . . . 乱数発生ユニット, 2 3 3 . . . 暗号化ユニット, 2 4 1 . . . 相互認証モジュール, 2 4 2 . . . 復号モジュール, 2 4 3 . . . 復号モジュール, 2 4 4 . . . 伸張モジュール, 2 4 5 . . . ウォータマーク付加モジュール

This Page Blank (uspto)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/02290

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F17/60, G06F13/00, G09C1/00, H04L9/08, G06F15/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Toroku Jitsuyo Shinan Koho 1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST File (JOIS)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO, 96/27155, A2 (InerTrust Technologies Corp.), 06 September, 1996 (06.09.96) & JP, 10-512074, A	1-8
Y	Jinbun Kagaku to Computer, Vols. 36 to 38, November, 1997, Seiji Kawahara, "Chosaku Ken Shori Gijutsu no Saikin no Doko", pp.43-48	1-8

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not

considered to be of particular relevance

"E" earlier document but published on or after the international filing

date

"L" document which may throw doubts on priority claim(s) or which is

cited to establish the publication date of another citation or other

special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other

means

"P" document published prior to the international filing date but later

than the priority date claimed

"T" later document published after the international filing date or

priority date and not in conflict with the application but cited to

understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be

considered novel or cannot be considered to involve an inventive

step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be

considered to involve an inventive step when the document is

combined with one or more other such documents, such

combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

24 May, 2000 (24.05.00)

Date of mailing of the international search report

13 June, 2000 (13.06.00)

Name and mailing address of the ISA/

Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

This Page Blank (uspto)

国際調査報告

国際出願番号 PCT/JPO0/02290

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl¹ G06F17/60

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl¹ G06F17/60 G06F13/00 G09C1/00 H04L9/08 G06F15/00 H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年
 日本国公開実用新案公報 1971-2000年
 日本国実用新案登録公報 1996-2000年
 日本国登録実用新案公報 1994-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル(JOIS)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	WO, 96/27155, A2 (InerTrust Technologies Corp.) 6. 9月. 1996 (06. 09. 96) & JP, 10-512074, A	1-8
Y	人文科学とコンピュータ, 第36-8巻, 11月. 1997 河原正治「著作権処理技術の最近の動向」 p. 43-48	1-8

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

24. 05. 00

国際調査報告の発送日

13. 06. 00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

岩間 直純



5L

9287

電話番号 03-3581-1101 内線 3562

This Page Blank (uspto)